

Repair Optimal Erasure Codes through Hadamard Designs

Dimitris S. Papailiopoulos and Alexandros G. Dimakis
 Electrical Engineering
 University of Southern California
 Los Angeles, CA 90089
 Email: {papailio, dimakis}@usc.edu

Viveck R. Cadambe
 Electrical Engineering and Computer Science
 University of California Irvine,
 Irvine, CA, 92697
 Email: vcadambe@uci.edu

Abstract

In distributed storage systems that employ erasure coding, the issue of minimizing the total *communication* required to exactly rebuild a storage node after a failure arises. This repair bandwidth depends on the structure of the storage code and the repair strategies used to restore the lost data. Designing high-rate maximum-distance separable (MDS) codes that achieve the optimum repair communication has been a well-known open problem. In this work, we use Hadamard matrices to construct the first explicit 2-parity MDS storage code with optimal repair properties for all single node failures, including the parities. Our construction relies on a novel method of achieving perfect interference alignment over finite fields with a finite file size, or number of extensions. We generalize this construction to design m -parity MDS codes that achieve the optimum repair communication for single systematic node failures and show that there is an interesting connection between our m -parity codes and the systematic-repair optimal permutation-matrix based codes of Tamo *et al.* [21] and Cadambe *et al.* [22], [23].

I. INTRODUCTION

Distributed storage systems have reached such a massive scale that recovery from failures is now part of regular operation rather than a rare exception [4]. Large scale deployments typically need to tolerate multiple failures, both for high availability and to prevent data loss. Erasure coded storage achieves high failure tolerance without requiring a large number of replicas that increase the storage cost. Three application contexts where erasure coding techniques are being currently deployed or under investigation are Cloud storage systems [5], archival storage, and peer-to-peer storage systems like Cleversafe and Wuala.

One central problem in erasure coded distributed storage systems is that of maintaining an encoded representation when failures occur. To maintain the same redundancy when a storage node leaves the system, a *newcomer* node has to join the array, access some existing nodes, and exactly reproduce the contents of the departed node. In its most general form this problem is known as the *Exact Code Repair Problem* [2], [1]. There are several metrics that can be optimized during repair: the total information read from existing disks during repair [8], [9], the total information communicated in the network (repair bandwidth [2]), or the total number of disks required for each repair [5], [10], [21], [23].

Currently, the most well-understood metric is that of repair bandwidth. For designing (n, k) MDS erasure codes that have n storage nodes and can tolerate any $n - k$ failures, the information theoretic cut-set bounds for repair communication were specified in [2] and shown to be achievable for all values of n, k in a series of recent papers [3], [13], [16], [18]–[20]. In particular, it was shown that for a (n, k) code, if a single node fails, downloading $\frac{1}{n-k}$ fraction of every surviving disk is sufficient and optimal in terms of repair bandwidth for the repair of a failed node. Beyond MDS codes, [2] demonstrated a tradeoff between storage and repair communication, and code constructions for other points of this tradeoff are under active investigation, see e.g. [3], [20], or [24] for multiple node repair schemes. On this tradeoff, the minimum storage point is achieved by MDS erasure codes with optimal repair, also known as Minimum Storage Regenerating (MSR) codes.

For code rates $k/n \leq 1/2$, explicit MSR codes were designed by Shah *et al.* [16], Rashmi *et al.* [20], and Suh *et al.* [15]. For the high-rate regime, however, the only known complete constructions [18], [19] require large file sizes (symbol extensions) and field sizes. These constructions use the symbol extension interference alignment (IA) technique of [11] to establish that there exist MDS storage codes, that come arbitrarily close to (but do not exactly match) the information theoretic lower bound for the repair bandwidth for all n, k . These asymptotic constructions are impractical due to the arbitrarily large finite field size and the fast growing file size, required even for small values of n and k .

Our Contribution: We introduce the first explicit high-rate $(k+2, k)$ MDS storage code with optimal repair communication. Our storage code exploits fundamental properties of Hadamard designs and perfect IA instances that can be understood through the use of a lattice representation of the symbol extension technique of Cadambe *et al.* [11], [18], [19]. Our coding and repair strategy bears resemblance to the notion of ergodic interference alignment [25], which is a finite-symbol-extension based IA scheme in the wireless channels.

Independently of this work, there has recently been a substantial progress in designing high-rate explicit MSR codes. Tamo *et al.* [21] and Cadambe *et al.* [23] designed MDS codes for any (n, k) parameters that have optimal repair for the systematic nodes, but not the code parities. It seems that extending these designs to allow optimal parity repair is not straightforward.

The advantage of our work is that all n nodes are optimally repaired and the disadvantage is that our construction is currently only optimal for $n - k = 2$.

Our key technical contribution is a scheme that achieves *perfect* interference alignment with a finite number of extensions. This was developed in [26] and used in 2 parity storage code with optimal repair for k nodes and near optimal repair of 2 nodes, that can handle any single node failure. We use a combinatorial view of different interference alignment schemes using a framework we call dots-on-a-lattice. Hadamard matrices are shown to be crucial in achieving finite perfect alignment and ensuring the full-rank of desired subspaces.

Finally, we present m -parity MDS code constructions based on Hadamard designs that achieve optimal repair for systematic node failures, but suboptimal repair for parity nodes. We show that these codes are equivalent to codes that involve permutation matrices in the manner of [21] and [23] under a similarity transformation.

2-parity Code Parameters: Assuming that the file to be encoded has size $M = k2^{k+1}$, each of the $k + 2$ storage nodes stores a coded block of size $\frac{M}{k}$. Repairing a single node failure costs $\frac{k+1}{2k}M$ in repair communication bandwidth, matching the theoretic lower bound. Finally, we give explicit conditions on the MDS property of the code and show that finite fields of size greater than or equal to $2k + 3$ suffice to satisfy them.

m-parity Code Parameters: For file sizes $M = km^k$, our $(k + m, k)$ codes achieve a repair communication bandwidth of $\frac{k+m-1}{mk}M$ for single systematic node failures, matching the information theoretic lower bound. The MDS property of these codes is shown to hold for arbitrarily large finite fields with high probability.

II. MDS STORAGE CODES WITH 2 PARITY NODES

In this section, we consider the code repair problem for MDS storage codes with 2 parity nodes. After we lay down the model for repair, we continue with introducing our code construction. Let a file of size $M = kN$ denoted by the vector $\mathbf{f} \in \mathbb{F}_q^{kN}$ be partitioned in k parts $\mathbf{f} = [\mathbf{f}_1^T \dots \mathbf{f}_k^T]^T$, each of size N , where N denotes the subpacketization factor, $\frac{N}{2} \in \mathbb{N}^*$.¹ We wish to store \mathbf{f} across k systematic and 2 parity storage units each having storage capacity $\frac{M}{k} = N$, hence we consider a data rate of $\frac{k}{k+2}$. We require that the encoded storage array is resilient up to any 2 node erasures. To satisfy the redundancy and erasure resiliency properties, the file is encoded using a $(k + 2, k)$ MDS distributed storage code. A storage code has the MDS property when any possible collections of k storage nodes can reconstruct the file \mathbf{f} .

systematic node	systematic data
1	\mathbf{f}_1
\vdots	\vdots
k	\mathbf{f}_k
parity node	parity data
1	$\mathbf{f}_1 + \dots + \mathbf{f}_k$
2	$\mathbf{A}_1^T \mathbf{f}_1 + \dots + \mathbf{A}_k^T \mathbf{f}_k$

Fig. 1. A $(k + 2, k)$ CODED STORAGE ARRAY.

In Fig. 1 we provide a general structure of a two parity MDS encoded storage array. The first k storage nodes store the systematic file parts. Without loss of generality, the first parity stores the sum of all k systematic parts $\mathbf{f}_1 + \dots + \mathbf{f}_k$ and the second parity stores a linear combination of them $\mathbf{A}_1^T \mathbf{f}_1 + \dots + \mathbf{A}_k^T \mathbf{f}_k$. Here, \mathbf{A}_i denotes an $N \times N$ matrix of coding coefficients used by the second parity node to “scale and mix” the contents of the i th file piece \mathbf{f}_i , $i \in \{1, \dots, k\}$. This representation is a systematic one: k nodes store uncoded file pieces and each of the 2 parities stores a linear combination of the k file parts.

In this work, we are interested in maintaining the same level of redundancy when a storage component fails or leaves the system. To do that the *code repair* process has to take place to exactly regenerate the lost data in a *newcomer* storage component. Let, for example, a systematic node $i \in \{1, \dots, k\}$ fail. Then, a newcomer joins the storage network, connects to the remaining nodes, and has to download sufficient data to reconstruct \mathbf{f}_i .

It is important to note that the lost systematic part \mathbf{f}_i , exists *only* as a term of a linear combination at each parity node, as seen in Fig. 1. Therefore, to regenerate the N elements of \mathbf{f}_i , the newcomer has to download from the parity nodes a size of data equal to the size of the lost piece, i.e., N linearly independent coded elements. Assuming that it downloads the same amount of data from both parities, the downloaded contents can be represented as a stack of N equations

$$\begin{bmatrix} \mathbf{p}_i^{(1)} \\ \mathbf{p}_i^{(2)} \end{bmatrix} \triangleq \begin{bmatrix} (\mathbf{V}_i^{(1)})^T \mathbf{f}_1 + \dots + (\mathbf{V}_i^{(1)})^T \mathbf{f}_k \\ (\mathbf{V}_i^{(2)})^T \mathbf{A}_1^T \mathbf{f}_1 + \dots + (\mathbf{V}_i^{(2)})^T \mathbf{A}_k^T \mathbf{f}_k \end{bmatrix} = \underbrace{\begin{bmatrix} (\mathbf{V}_i^{(1)})^T \\ (\mathbf{A}_i \mathbf{V}_i^{(2)})^T \end{bmatrix}}_{\text{useful data}} \mathbf{f}_i + \sum_{s=1, s \neq i}^k \underbrace{\begin{bmatrix} (\mathbf{V}_i^{(1)})^T \\ (\mathbf{A}_s \mathbf{V}_i^{(2)})^T \end{bmatrix}}_{\text{interference by } \mathbf{f}_s} \mathbf{f}_s, \quad (1)$$

¹ \mathbb{F}_q denotes the finite field, over which all operation are performed.

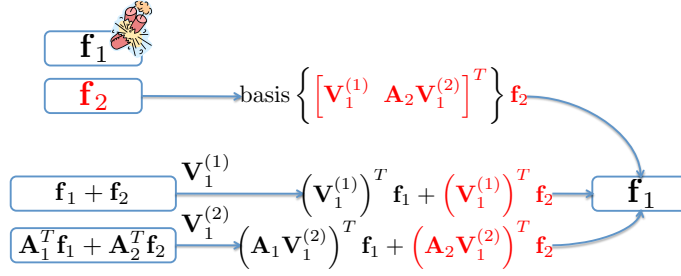


Fig. 2. Repair of a $(4, 2)$ code. Let systematic node 1 fail. Then, a newcomer node joins the system and downloads data from the 3 remaining nodes to regenerate \mathbf{f}_1 . The useful information is mixed with the undesired part \mathbf{f}_2 in both information chunks downloaded from the parities. These interference parts are highlighted in red. To retrieve \mathbf{f}_1 a basis of the interference equations needs to be downloaded by systematic node 2. Then, the newcomer can erase interference and invert the matrix multiplying \mathbf{f}_1 to retrieve it. Note that for invertibility, we need the additional condition that the matrix $\begin{bmatrix} \mathbf{V}_1^{(1)} & \mathbf{A}_1 \mathbf{V}_1^{(2)} \end{bmatrix}^T$ has a full rank of N .

where $\mathbf{p}_i^{(1)}, \mathbf{p}_i^{(2)} \in \mathbb{F}_q^{\frac{N}{2}}$ are the equations downloaded from the first and second parity node, respectively, and $\mathbf{V}_i^{(1)}, \mathbf{V}_i^{(2)} \in \mathbb{F}_q^{N \times \frac{N}{2}}$ are the *repair matrices*. Each repair matrix is used to mix the N parity contents so that a set of $\frac{N}{2}$ equations is formed. Then, retrieving \mathbf{f}_i from (1) is equivalent to solving an underdetermined set of N equations in the kN unknowns of \mathbf{f} , with respect to the N desired unknowns of \mathbf{f}_i . However, this is not possible due to $k-1$ additive *interference* components in the received equations generated by the undesired unknowns \mathbf{f}_s , $s \in \{1, \dots, k\} \setminus i$, as noted in (1). These $k-1$ interference terms corrupt the desired data and need to be canceled. Hence, the newcomer needs to download additional data from the remaining $k-1$ systematic nodes, that will “replicate” and cancel the interference terms from the downloaded equations.

To cancel a single interference term of (1) that has size N , it suffices to download a basis of equations that generates it. The dimensions of this basis does not need to be equal to N . For example, to erase

$$\begin{bmatrix} (\mathbf{V}_i^{(1)})^T \\ (\mathbf{A}_s \mathbf{V}_i^{(2)})^T \end{bmatrix} \mathbf{f}_s, \quad s \in \{1, \dots, k\} \setminus i \quad (2)$$

the newcomer needs to connect to systematic node s and download a number of linear equations in \mathbf{f}_s that can generate (2); this number is equal to

$$\frac{N}{2} \leq \text{rank} \left(\begin{bmatrix} (\mathbf{V}_i^{(1)})^T \\ (\mathbf{A}_s \mathbf{V}_i^{(2)})^T \end{bmatrix} \right) \leq N, \quad (3)$$

This is exactly the communication bandwidth price we are paying to delete a single interference term in order to be able to reconstruct \mathbf{f}_i . The lower bound in (3) comes from the fact that $\frac{N}{2}$ linearly independent equations need to be downloaded from each of the parities, hence $\text{rank}(\mathbf{V}_i^{(1)}) = \text{rank}(\mathbf{V}_i^{(2)}) = \frac{N}{2}$ for any $i \in \{1, \dots, k\}$. Eventually, we need to generate all undesired terms in the newcomer, so to subtract them from (1). Then, a full rank system of N equations in the N unknowns has to be formed. A generic example of a code repair instance for a $(4, 2)$ storage code is given in Fig. 2.

In general, to repair a systematic node $i \in \{1, \dots, k\}$ of an arbitrary $(k+2, k)$ MDS storage code, we need to obtain a feasible solution to the following rank constrained, rank minimization (performed over \mathbb{F}_q)

$$\begin{aligned} \mathcal{R}_i: \quad & \min_{\mathbf{V}_i^{(1)}, \mathbf{V}_i^{(2)}} \sum_{s=1, s \neq i}^k \text{rank} \left(\begin{bmatrix} \mathbf{V}_i^{(1)} & \mathbf{A}_s \mathbf{V}_i^{(2)} \end{bmatrix} \right) \\ \text{s.t.:} \quad & \text{rank} \left(\begin{bmatrix} \mathbf{V}_i^{(1)} & \mathbf{A}_i \mathbf{V}_i^{(2)} \end{bmatrix} \right) = N, \end{aligned}$$

where *i*) the full rank constraints correspond to the requirement that the N equations downloaded from the parities are linearly independent, when viewed as equations in the N components of \mathbf{f}_i and *ii*) the rank minimization corresponds to minimizing the sum of bases dimensions needed to cancel each interference term. For a specific feasible selection of repair matrices the *repair bandwidth* to exactly regenerate systematic node i is given by

$$\gamma_i = \underbrace{N}_{\text{\#equations lost}} + \sum_{s=1, s \neq i}^k \underbrace{\text{rank} \left(\begin{bmatrix} \mathbf{V}_i^{(1)} & \mathbf{A}_s \mathbf{V}_i^{(2)} \end{bmatrix} \right)}_{\text{dim. of interference equations by } \mathbf{f}_s} = N + \sum_{s=1, s \neq i}^k \text{rank} \left(\begin{bmatrix} \mathbf{V}_i^{(1)} & \mathbf{A}_s \mathbf{V}_i^{(2)} \end{bmatrix} \right), \quad (4)$$

where the sum rank term is the aggregate of interference dimensions. An optimal solution to \mathcal{R}_i is guaranteed to minimize the repair bandwidth we need to communicate to the repair systematic node $i \in \{1, \dots, k\}$.

[illegible]

Fig. 3. A repair optimal $(5, 3)$ MDS code over \mathbb{F}_{11}

Remark 1: From [2] it is known that the theoretical minimum repair bandwidth, for any single node repair of an optimal (linear or nonlinear) $(k+2, k)$ MDS code is exactly $(k+1)\frac{N}{2}$, where N has to be an even number. This bound is proven using cut-set bounds on infinite flow graphs. Here, we provide an interpretation of this bound in terms of linear codes by calculating the minimum possible sum of ranks in \mathcal{R}_i : since each repair matrix *has* to have full column rank $\frac{N}{2}$ to be a feasible solution, the minimum number of dimensions each interference can be suppressed to is $\frac{N}{2}$. This aggregates in a minimum repair bandwidth of $(k+1)\frac{N}{2}$ repair equations. If we wish to achieve this bound, *interference alignment* has to be employed, so that undesired components like (2) are confined to the minimum number of dimensions. Interestingly, linear codes suffice to asymptotically achieve this bound [18], [19].

We know what the theoretical minimum repair bandwidth is and that there exist asymptotically optimal schemes, however, designing MDS codes with repair strategies that achieve it has been challenging. The difficulty in designing optimal MDS storage codes lies in a threefold requirement: *i*) the code has to satisfy the MDS property, *ii*) systematic nodes of the code have to be optimally repaired, and *iii*) parity nodes of the code have to be optimally repaired. Currently, there exist MDS codes for rates $\frac{k}{n} \leq \frac{1}{2}$ [15], [20] for which all nodes can be optimally repaired. For the high data rate regime, Tamo *et al.* [21] and Cadambe *et al.* [23] presented the first MDS codes where any systematic node failure can be optimally repaired. However, prior to this work, there do not exist MDS storage codes of arbitrarily high rate that can optimal repair *any* node.

In the following, we present the first explicit, high-rate, repair optimal $(k + 2, k)$ MDS storage code that achieves the minimum repair bandwidth bound for the repair of *any* single systematic or parity node failure.

III. A REPAIR OPTIMAL 2 PARITY STORAGE CODE

Let a $(k+2, k)$ MDS storage code for file size $M = k2^{k+1}$, with coding matrices

$$\mathbf{A}_i = a_i \mathbf{X}_i + b_i \mathbf{X}_{k+1} + \mathbf{I}_N, \quad i \in \{1, \dots, k\} \quad (5)$$

where $N = 2^{k+1}$,

$$\mathbf{X}_i = \mathbf{I}_{2^{i-1}} \otimes \text{blkdiag} \left(\mathbf{I}_{\frac{N}{2^k}}, -\mathbf{I}_{\frac{N}{2^k}} \right), \quad (6)$$

and a_i, b_i satisfy $a_i^2 - b_i^2 = -1$, for all $i \in \{1, \dots, k\}$.²

Theorem 1: There exists a finite field \mathbb{F}_q of order $q \geq 2k + 3$ and explicit constants $a_i, b_i \in \mathbb{F}_q$, $\forall i \in \{1, \dots, k\}$, such that the $(k, k + 2)$ storage code in (5) is a repair optimal MDS storage code.

In Fig. 3, we give the coding matrices of a $(5, 3)$ MDS code over \mathbb{F}_{11} based on our construction.

Remark 2: The code constructions presented here have generator matrices that are as sparse as possible, since any additional sparsity would violate the MDS property. This creates the additional benefit of minimum update complexity when some bits of the stored data object change.

Before we proceed with proving Theorem 1, we state the intuition behind our code construction and the tools that we use. Motivated by the asymptotic IA schemes, we use similar concepts motivated by a combinatorial explanation of interference alignment in terms of dots on lattices. In contrast to the asymptotic IA codes, here, instead of letting randomness choose the coding matrices, we select particular constructions based on Hadamard matrices that achieve *exact* interference alignment for fixed in k file sizes (symbol extensions). In section V we prove the optimal repair of systematic nodes, in Section VII we show the optimal repair of parity nodes, and in section VIII we state explicit conditions for the MDS property.

²We use -1 to denote the field element $q - 1$ over \mathbb{F}_q .

IV. DOTS-ON-A-LATTICE AND HADAMARD DESIGNS

In Section II, we showed that minimizing the communication bandwidth to repair nodes of a storage code is equivalent to the problem of minimizing the dimensions of interference terms generated during each repair process. Here, we consider the problem of designing coding and repair matrices that can achieve *perfect* interference alignment in a finite number of extensions. We begin by assuming arbitrary constructions and then we use a combinatorial explanation of IA to find conditions under which perfect alignment in the finite file regime. Eventually, we show that exact IA conditions and linear independence requirements posed by our problem are simultaneously satisfied through the use of Hadamard designs.

Assume two arbitrary $N \times N$ full rank matrices \mathbf{T}_1 and \mathbf{T}_2 that commute. We wish to construct a full rank matrix \mathbf{V} , with at most $\frac{N}{2}$ columns, such that the span of $\mathbf{T}_1\mathbf{V}$ aligns as much as possible with the span of $\mathbf{T}_2\mathbf{V}$: we have to pick \mathbf{V} such that it minimizes the dimensions of the union of the two spans, that is the rank of $[\mathbf{T}_1\mathbf{V} \ \mathbf{T}_2\mathbf{V}]$. How can we construct such a matrix? Assume that we start with one vector with nonzero entries, i.e., $\mathbf{V} = \mathbf{w}$, and for simplicity we let it be the all-ones vector. Then in the general case, $\mathbf{T}_1\mathbf{w}$ and $\mathbf{T}_2\mathbf{w}$ have zero intersection which is not desired. However, we can augment \mathbf{V} such that it has as columns the elements of the set $\{\mathbf{w}, \mathbf{T}_1\mathbf{w}, \mathbf{T}_2\mathbf{w}, \mathbf{T}_1\mathbf{T}_2\mathbf{w}\}$. Observe that each vector $\mathbf{T}_1^{x_1}\mathbf{T}_2^{x_2}\mathbf{w}$ of \mathbf{V} can be represented by the power tuple (x_1, x_2) . This helps us visualize \mathbf{V} as a set of dots on the 2-dimensional integer lattice as shown in Fig. 4.

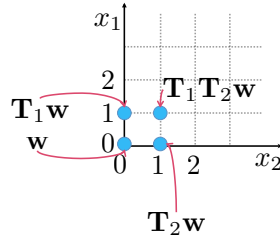


Fig. 4. Representing \mathbf{V} as dots on a lattice.

For this new selection of \mathbf{V} , we have

$$\mathbf{T}_1\mathbf{V} = [\mathbf{T}_1\mathbf{w} \ \mathbf{T}_1^2\mathbf{w} \ \mathbf{T}_1\mathbf{T}_2\mathbf{w} \ \mathbf{T}_1^2\mathbf{T}_2\mathbf{w}] \quad (7)$$

$$\text{and } \mathbf{T}_2\mathbf{V} = [\mathbf{T}_2\mathbf{w} \ \mathbf{T}_2\mathbf{T}_1\mathbf{w} \ \mathbf{T}_2^2\mathbf{w} \ \mathbf{T}_1\mathbf{T}_2^2\mathbf{w}]. \quad (8)$$

The intersection of the spans of these two matrices is now nonzero: the matrix $[\mathbf{T}_1\mathbf{V} \ \mathbf{T}_2\mathbf{V}]$ has rank 7 instead of the maximum possible of 8. This happens because the vector $\mathbf{T}_1\mathbf{T}_2\mathbf{w}$ is repeated in both matrices $\mathbf{T}_1\mathbf{V}$ and $\mathbf{T}_2\mathbf{V}$. In Fig. 5 we illustrate this concatenation, in terms of dots on \mathbb{Z}^2 , where the intersection between the two spans is manifested as an overlap of dots.

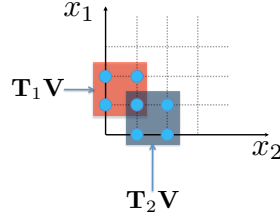


Fig. 5. Representing $[\mathbf{T}_1\mathbf{V} \ \mathbf{T}_2\mathbf{V}]$ as dots on a lattice.

Remark 3: Observe how matrix multiplication of \mathbf{T}_1 and \mathbf{T}_2 with the vectors in \mathbf{V} is pronounced through the dots representation: the dots representations of $\mathbf{T}_1\mathbf{V}$ and $\mathbf{T}_2\mathbf{V}$ matrices are shifted versions of \mathbf{V} along the x_1 and x_2 axes. The key idea behind choosing a new \mathbf{V} at each step is to iteratively augment the old one with products of the \mathbf{T}_i matrices raised to specific powers times the current \mathbf{V}

$$\text{initialize : } \mathbf{V} \leftarrow \mathbf{w} \quad (9)$$

$$\text{multiply with powers of } \mathbf{T}_1: \mathbf{V} \leftarrow [\mathbf{V} \ \mathbf{T}_1\mathbf{V} \dots \mathbf{T}_1^{m-1}\mathbf{V}] \quad (10)$$

$$\text{multiply with powers of } \mathbf{T}_2: \mathbf{V} \leftarrow [\mathbf{V} \ \mathbf{T}_2\mathbf{V} \dots \mathbf{T}_2^{m-1}\mathbf{V}]. \quad (11)$$

In general, by using powers up to m , with $m^2 \leq \frac{N}{2}$, we obtain \mathbf{V} with m^2 columns that are the elements of the set

$$\mathcal{V} = \{\mathbf{T}_1^{x_1}\mathbf{T}_2^{x_2}\mathbf{w} : x_s \in \{0, \dots, m-1\}\}, \quad (12)$$

where $\mathbf{w} = \mathbf{1}_{N \times 1}$. Then, matrix \mathbf{V} achieves the following property

$$m^2 < \text{rank}([\mathbf{T}_1 \mathbf{V} \quad \mathbf{T}_2 \mathbf{V}]) < (m+1)^2, \quad (13)$$

which means that we can asymptotically create as much alignment as we desire within the spans of the matrices $\mathbf{T}_i \mathbf{V}$, for arbitrarily large “symbol extensions”, i.e. for sufficiently large N , $(m+1)^2/m^2$ is arbitrarily close to 1. For example, we give the $m = 4$ case in Fig. 6, where we observe that the alignment is more substantial (with respect to the size of \mathbf{V}) compared to Fig. 5. This alignment scheme, in a more general form, was presented by Cadambe and Jafar in [11] to prove

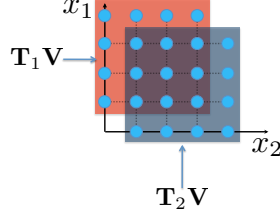


Fig. 6. Representing $[\mathbf{T}_1 \mathbf{V} \quad \mathbf{T}_2 \mathbf{V}]$ as dots on a lattice.

the Degrees-of-Freedom of the K -user interference channel. For that wireless scenario, the \mathbf{T}_i matrices are given by nature and are i.i.d. diagonals. Perfect alignment of spaces for these matrices is not known to be possible for finite m [11], [28].

For network coding problems, and in particular, for storage coding problems, the analogous \mathbf{T}_i matrices (our coding matrices) are free to design under some specific constraints that ensure the MDS property of the code. Before, we give explicit matrices that achieve alignment in a finite number of extensions, we answer the analogous question considering our toy example: do there exist \mathbf{T}_1 and \mathbf{T}_2 matrices such that we can construct a full-rank \mathbf{V} that achieves perfect intersection (exact alignment) of the spans of $\mathbf{T}_1 \mathbf{V}$ and $\mathbf{T}_2 \mathbf{V}$, for some m and $N = m^3$? That is, can we find matrices such that

$$\text{span}(\mathbf{T}_1 \mathbf{V}) = \text{span}(\mathbf{T}_2 \mathbf{V}) \text{ and } \text{rank}(\mathbf{V}) = m^2 \quad (14)$$

is possible? We show that a sufficient condition for perfect alignment is satisfied when the elements of the matrices are m^{th} roots of unity, i.e.,

$$\mathbf{T}_i^m = \mathbf{I}_N. \quad (15)$$

To see, that we formally state the dots on a lattice representation. Let a map \mathcal{L} from a matrix with r columns, each generated as $\mathbf{T}_1^{x_1} \mathbf{T}_2^{x_2} \mathbf{w}$, to a set of r points, such that the column $\mathbf{T}_1^{x_1} \mathbf{T}_2^{x_2} \mathbf{w}$ maps to the point (x_1, x_2) . Then, we have for \mathbf{V}

$$\mathcal{L}(\mathbf{V}) \triangleq \{x_1 \mathbf{e}_1 + x_2 \mathbf{e}_2; x_1, x_2 \in [m]\}, \quad (16)$$

where $[m] = \{0, \dots, m-1\}$ and \mathbf{e}_i is the i -th column of the identity matrix. Using this representation, the products $\mathbf{T}_1 \mathbf{V}$ and $\mathbf{T}_2 \mathbf{V}$ map to

$$\mathcal{L}(\mathbf{T}_1 \mathbf{V}) = \{(x_1 + 1) \mathbf{e}_1 + x_2 \mathbf{e}_2 : x_1, x_2 \in [m]\} \text{ and } \mathcal{L}(\mathbf{T}_2 \mathbf{V}) = \{x_1 \mathbf{e}_1 + (x_2 + 1) \mathbf{e}_2 : x_1, x_2 \in [m]\} \quad (17)$$

respectively. For perfect alignment, we have to design the \mathbf{T}_i matrices such that

$$\mathcal{L}(\mathbf{T}_1 \mathbf{V}) = \mathcal{L}(\mathbf{T}_2 \mathbf{V}). \quad (18)$$

A sufficient set of conditions for perfect span intersection is that \mathbf{V} , $\mathbf{T}_1 \mathbf{V}$, and $\mathbf{T}_2 \mathbf{V}$ perfectly intersect, i.e.

$$\mathcal{L}(\mathbf{T}_1 \mathbf{V}) = \mathcal{L}(\mathbf{V}) \Leftrightarrow \{(x_1 + 1) \mathbf{e}_1 + x_2 \mathbf{e}_2 : x_1, x_2 \in [m]\} = \{x_1 \mathbf{e}_1 + x_2 \mathbf{e}_2 : x_1, x_2 \in [m]\}, \quad (19)$$

$$\mathcal{L}(\mathbf{T}_2 \mathbf{V}) = \mathcal{L}(\mathbf{V}) \Leftrightarrow \{x_1 \mathbf{e}_1 + (x_2 + 1) \mathbf{e}_2 : x_1, x_2 \in [m]\} = \{x_1 \mathbf{e}_1 + x_2 \mathbf{e}_2 : x_1, x_2 \in [m]\}. \quad (20)$$

The above conditions are satisfied when the matrix powers “wrap around” upon reaching a certain modulus m . This wrap-around property is obtained when the \mathbf{T}_1 and \mathbf{T}_2 matrices have elements that are m^{th} roots of unity

$$\mathbf{T}_1^m = \mathbf{T}_1^0 = \mathbf{T}_2^m = \mathbf{T}_2^0 = \mathbf{I}_N. \quad (21)$$

However, arbitrary diagonal matrices whose elements are m^{th} roots of unity are not sufficient to ensure the full rank property of \mathbf{V} . To hint on a general procedure which outputs “good” \mathbf{T}_i matrices, we see an example where we pick them such that \mathbf{V} has orthogonal columns. Let us briefly consider the case where $m = 2$ and $N = 2^3$, for which we choose

$$\mathbf{T}_1 = \text{diag} \left(\begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \\ 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} \right) \quad \text{and} \quad \mathbf{T}_2 = \text{diag} \left(\begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \\ 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} \right). \quad (22)$$

For these matrices, \mathbf{V} has $m^2 = 4$ orthogonal columns

$$\mathbf{V} = [\mathbf{w} \quad \mathbf{T}_1 \mathbf{w} \quad \mathbf{T}_2 \mathbf{w} \quad \mathbf{T}_1 \mathbf{T}_2 \mathbf{w}] = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \quad (23)$$

and $\mathbf{T}_2 \mathbf{V} = [\mathbf{T}_2 \mathbf{w} \quad \mathbf{T}_1 \mathbf{T}_2 \mathbf{w} \quad \mathbf{w} \quad \mathbf{T}_1 \mathbf{w}]$, $\mathbf{T}_3 \mathbf{V} = [\mathbf{T}_1 \mathbf{w} \quad \mathbf{w} \quad \mathbf{T}_1 \mathbf{T}_2 \mathbf{w} \quad \mathbf{T}_2 \mathbf{w}]$ indeed have fully overlapping spans. Interestingly, we observe that for the additional matrix

$$\mathbf{T}_3 = \text{diag} \left(\begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \\ -1 \\ -1 \\ -1 \\ -1 \end{bmatrix} \right) \quad (24)$$

we have that $[\mathbf{V} \quad \mathbf{T}_3 \mathbf{V}] = \mathbf{H}_8$, where \mathbf{H}_8 is the 8×8 Hadamard matrix. In the following we see that Hadamard designs provide the conditions for perfect alignment and linear independence in a more general setting.

Let $m = 2$, $N = 2^L$, and $\mathbf{X}_i = \mathbf{I}_{2^{i-1}} \otimes \text{blkdiag}(\mathbf{I}_{\frac{N}{2^i}}, -\mathbf{I}_{\frac{N}{2^i}})$, for $i \in [L]$, and consider the set

$$\mathcal{H}_N = \left\{ \prod_{i=1}^L \mathbf{X}_i^{x_i} \mathbf{w} : x_i \in \{0, 1\} \right\}. \quad (25)$$

Lemma 1: Let an $N \times N$ Hadamard matrix of the Sylvester’s construction

$$\mathbf{H}_N \triangleq \begin{bmatrix} \mathbf{H}_{\frac{N}{2}} & \mathbf{H}_{\frac{N}{2}} \\ \mathbf{H}_{\frac{N}{2}} & -\mathbf{H}_{\frac{N}{2}} \end{bmatrix}, \quad (26)$$

with $\mathbf{H}_1 = 1$. Then, \mathbf{H}_N is full rank with mutually orthogonal columns, that are the N elements of \mathcal{H}_N .

The proof of Lemma (1) can be found in the Appendix.

Example To illustrate the connection between \mathcal{H}_N and \mathbf{H}_N we “decompose” the Hadamard matrix of order 4

$$\mathbf{H}_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} = [\mathbf{w} \quad \mathbf{X}_2 \mathbf{w} \quad \mathbf{X}_1 \mathbf{w} \quad \mathbf{X}_2 \mathbf{X}_1 \mathbf{w}], \quad (27)$$

where $\mathbf{X}_1 = \text{diag} \left(\begin{bmatrix} 1 \\ -1 \end{bmatrix} \right)$ and $\mathbf{X}_2 = \text{diag} \left(\begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} \right)$. Due to the commutativity of \mathbf{X}_1 and \mathbf{X}_2 , the columns of \mathbf{H}_4 are also the elements of $\mathcal{H}_4 = \{\mathbf{w}, \mathbf{X}_1 \mathbf{w}, \mathbf{X}_2 \mathbf{w}, \mathbf{X}_1 \mathbf{X}_2 \mathbf{w}\}$.

Now, consider the matrix \mathbf{V}_i that has as columns the elements of

$$\mathcal{V}_i = \left\{ \prod_{s=1, s \neq i}^L \mathbf{X}_s^{x_s} \mathbf{w} : x_s \in \{0, 1\} \right\}. \quad (28)$$

We know that the space of \mathbf{V}_i is invariant with respect to \mathbf{X}_j since the corresponding lattice representation wraps around itself due to $\mathbf{X}_i^2 = \mathbf{I}_N$. Additionally, we have

$$\mathcal{L}(\mathbf{X}_i \mathbf{V}_i) = \left\{ \mathbf{e}_i + \sum_{s=1, s \neq i}^L x_s \mathbf{e}_s : x_s \in \{0, 1\} \right\},$$

and we observe that $\mathcal{L}(\mathbf{X}_i \mathbf{V}_i) \cap \mathcal{L}(\mathbf{V}_i) = \emptyset$, i.e., $\mathcal{L}(\mathbf{V}_i)$ does not include any points with nonzero x_i coordinates. Then, due to the orthogonality of elements within \mathcal{H}_N , we have

$$|\mathcal{L}(\mathbf{V}_i)| = |\mathcal{L}(\mathbf{X}_j \mathbf{V}_i)| = \text{rank}(\mathbf{V}_i) = \text{rank}(\mathbf{X}_i \mathbf{V}_i) = \frac{N}{2}, \quad (29)$$

for any $i, j \in \{1, \dots, L\}$. Hence, we obtain the following lemma for the set \mathcal{H}_N and its associated \mathcal{L} map.

Lemma 2: For any $i, j \in \{1, 2, \dots, L\}$ we have that

$$\text{rank}([\mathbf{V}_i \quad \mathbf{X}_j \mathbf{V}_i]) = |\mathcal{L}(\mathbf{V}_i) \cup \mathcal{L}(\mathbf{X}_j \mathbf{V}_i)| = \begin{cases} N, & i = j, \\ \frac{N}{2}, & i \neq j. \end{cases} \quad (30)$$

In Fig. 7 we give an illustrative example of the aforementioned definitions and properties. For $N = 2^3$, we consider \mathbf{H}_8 and \mathbf{V}_3 along with the matrix product $\mathbf{X}_2 \mathbf{V}_3$ and their corresponding lattice representations.

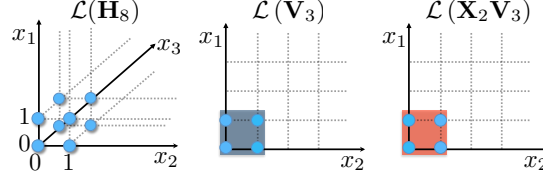


Fig. 7. We set $N = 8$ and show the dots representation of \mathbf{H}_8 , \mathbf{V}_3 , and $\mathbf{X}_2 \mathbf{V}_3$.

We use the aforementioned properties of Hadamard matrices to construct repair matrices \mathbf{V}_i for our code construction; these matrices have perfect space alignment properties for the repair instances of the code in (5) induced by single node failures.

Remark 4: Notice that equations (22) and (23) are respectively analogous to the channel matrices and beamforming vectors used in wireless channels for ergodic interference alignment [25]. In particular, for the K user interference channel, the channel matrices used for ergodic alignment are diagonalized versions of the column vectors of \mathbf{H}_2 .

V. OPTIMAL SYSTEMATIC NODE REPAIR

Let systematic node $i \in \{1, \dots, k\}$ of the code in (5) fail. The coding matrix \mathbf{A}_i corresponding to the lost systematic piece \mathbf{f}_i , holds one matrix, that is, \mathbf{X}_i , which is unique among all other coding matrices, \mathbf{A}_s , $s \in \{1, \dots, k\} \setminus i$. We pick the repair matrix as a set of $\frac{N}{2}$ vectors whose lattice representation is invariant to all \mathbf{X}_j s but to one key matrix: the unique \mathbf{X}_i component of \mathbf{A}_i . We construct the $N \times \frac{N}{2}$ repair matrix \mathbf{V}_i whose columns are the elements of the set

$$\mathcal{V}_i = \left\{ \prod_{s=1, s \neq i}^{k+1} \mathbf{X}_s^{x_s} \mathbf{w} : x_s \in \{0, 1\} \right\}. \quad (31)$$

This repair matrix is used to multiply both the contents of parity node 1 and 2, that is, $\mathbf{V}_i^{(1)} = \mathbf{V}_i^{(2)} = \mathbf{V}_i$. During the repair, the useful (desired signal) space populated by \mathbf{f}_i is

$$[\mathbf{V}_i \quad \mathbf{A}_i \mathbf{V}_i] \quad (32)$$

and the interference space due to file part \mathbf{f}_s , $s \in \{1, \dots, k\} \setminus i$, is

$$[\mathbf{V}_i \quad \mathbf{A}_s \mathbf{V}_i]. \quad (33)$$

Remember that an optimal solution to \mathcal{R}_i requires the useful space to have rank N and each of the interference spaces rank $\frac{N}{2}$. Observe that the following holds for each of the interference spaces

$$\begin{aligned} \frac{N}{2} &\leq \text{rank}([\mathbf{V}_i \quad (a_s \mathbf{X}_s + b_s \mathbf{X}_{k+1} + \mathbf{I}_N) \mathbf{V}_i]) \\ &\leq |\mathcal{L}(\mathbf{V}_i) \cup \mathcal{L}(\mathbf{X}_s \mathbf{V}_i) \cup \mathcal{L}(\mathbf{X}_{k+1} \mathbf{V}_i)| = |\mathcal{L}(\mathbf{V}_i)| = \frac{N}{2}, \end{aligned} \quad (34)$$

for $s \in \{1, \dots, k\} \setminus i$, since

$$\mathcal{L}(\mathbf{X}_s \mathbf{V}_i) = \mathcal{L}(\mathbf{V}_i), s \in \{1, \dots, k+1\} \setminus i. \quad (35)$$

Then, for the useful data space we have

$$\begin{aligned} N &\geq \text{rank}([\mathbf{V}_i \quad \mathbf{A}_i \mathbf{V}_i]) = \text{rank}([\mathbf{V}_i \quad (a_i \mathbf{X}_i + b_i \mathbf{X}_{k+1} + \mathbf{I}_N) \mathbf{V}_i]) \\ &\stackrel{(*)}{=} \text{rank}([\mathbf{V}_i \quad \mathbf{X}_i \mathbf{V}_i]) = |\mathcal{L}(\mathbf{V}_i) \cup \mathcal{L}(\mathbf{X}_i \mathbf{V}_i)| \\ &= |\mathcal{L}(\mathbf{H}_N)| = N, \end{aligned} \quad (36)$$

for any $a_i \neq 0$, where $(*)$ comes from the fact that $(a_i \mathbf{X}_i + b_i \mathbf{X}_{k+1} + \mathbf{I}_N) \mathbf{V}_i$ is a linear combination of columns from \mathbf{V}_i , $\mathbf{X}_{k+1} \mathbf{V}_i$, and $\mathbf{X}_i \mathbf{V}_i$. The column spaces of \mathbf{V}_i and $\mathbf{X}_{k+1} \mathbf{V}_i$ are identical, hence we can generate the columns of

$(a_i \mathbf{X}_i + b_i \mathbf{X}_{k+1} + \mathbf{I}_N) \mathbf{V}_i$ by linear combinations of the columns in $\mathbf{X}_i \mathbf{V}_i$ and in \mathbf{V}_i , however \mathbf{V}_i is already in the concatenation $[\mathbf{V}_i \ (a_i \mathbf{X}_i + b_i \mathbf{X}_{k+1} + \mathbf{I}_N) \mathbf{V}_i]$. This means that $[\mathbf{V}_i \ \mathbf{X}_i \mathbf{V}_i]$ and $[\mathbf{V}_i \ (a_i \mathbf{X}_i + b_i \mathbf{X}_{k+1} + \mathbf{I}_N) \mathbf{V}_i]$ have the same span.

Therefore, we are able to generate the minimum amount of interference and at the same time satisfy the full rank constraint of \mathcal{R}_i . The repair matrix in (31) is an optimal solution for \mathcal{R}_i and systematic node i can be optimally repaired by downloading $(k+1)\frac{N}{2}$ worth data equations, for all $i \in \{1, \dots, k\}$. In Fig. 8, we sketch the structure of our code. In each block of the second parity we denote the key matrices that comprise it. We select our repair matrix such that it “absorbs” all matrices but the key one. That way, interference aligns in half the dimensions, and the useful space spans all N dimensions.

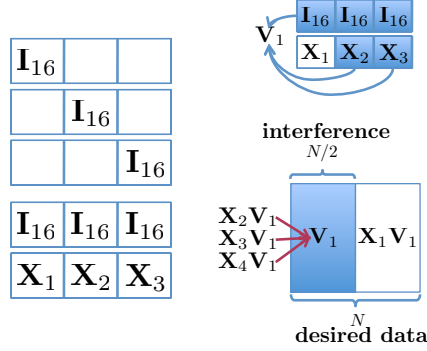


Fig. 8. A $(5, 3)$ repair optimal code.

VI. OPTIMAL PARITY REPAIR

The ingredient of our construction that “unlocks” optimal repair for the first parity is the inclusion of the identity matrix in each \mathbf{A}_i . The same goes for the \mathbf{X}_{k+1} matrix and the repair of the second parity. Both these additionally included matrices refine the parity repair process such that optimality is feasible. Selecting appropriate constants a_i and b_i is also essential to our developments. To optimally solve the problem, we rewrite the parity repair as a systematic one in an equivalent re-interpretation of our code.

A. Repairing the first parity

Let the first parity node fail. We make a change of variables to obtain a new representation for our code in (5), where the first parity is a systematic node in an equivalent representation. We start with our $(k, k+2)$ MDS storage code of (5)

$$\begin{bmatrix} \mathbf{I}_N & \mathbf{0}_N & \dots & \mathbf{0}_N \\ \mathbf{0}_N & \mathbf{I}_N & \dots & \mathbf{0}_N \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0}_N & \mathbf{0}_N & \dots & \mathbf{I}_N \\ \mathbf{I}_N & \mathbf{I}_N & \dots & \mathbf{I}_N \\ \mathbf{A}_1 & \mathbf{A}_2 & \dots & \mathbf{A}_k \end{bmatrix} \mathbf{f}. \quad (37)$$

and make the following change of variables

$$\sum_{i=1}^k \mathbf{f}_i = \mathbf{y}_1. \quad (38)$$

$$\mathbf{f}_s = \mathbf{y}_s, \quad s \in \{2, \dots, k\}. \quad (39)$$

We solve (38) and (39) for \mathbf{f}_1 in terms of the \mathbf{y}_i variables and obtain

$$\mathbf{f}_1 = \mathbf{y}_1 - \sum_{s=2}^k \mathbf{y}_s. \quad (40)$$

Then, we plug (39) and (40) in (37), to have the equivalent representation

$$\begin{bmatrix} \mathbf{I}_N & -\mathbf{I}_N & \dots & -\mathbf{I}_N \\ \mathbf{0}_N & \mathbf{I}_N & \dots & \mathbf{0}_N \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0}_N & \mathbf{0}_N & \dots & \mathbf{I}_N \\ \mathbf{I}_N & \mathbf{A}_2 - \mathbf{A}_1 & \dots & \mathbf{A}_k - \mathbf{A}_1 \end{bmatrix} \mathbf{y}, \quad (41)$$

where $\mathbf{y} = [\mathbf{y}_1^T \dots \mathbf{y}_k^T]^T \in \mathbb{F}_q^{kN}$. The first parity node of the code in (5) now corresponds to the node which contains \mathbf{y}_1 in the aforementioned representation. The coding matrices under this new representation are

$$\mathbf{A}_1 = a_1 \mathbf{X}_1 + b_1 \mathbf{X}_{k+1} + \mathbf{I}_N, \quad (42)$$

$$\mathbf{A}_s - \mathbf{A}_1 = a_s \mathbf{X}_s + (b_s - b_1) \mathbf{X}_{k+1} - a_1 \mathbf{X}_1, \quad (43)$$

for $s \in \{2, \dots, k\}$. In contrast to the systematic node repair process, in the following we use a repair matrix of a slightly different structure. We construct the repair matrix \mathbf{V}_a with columns in the set

$$\mathcal{V}_a = \left\{ \prod_{s=2}^{k+1} (\mathbf{X}_1 \mathbf{X}_s)^{x_s} \mathbf{w} : x_s \in \{0, 1\} \right\}. \quad (44)$$

Observe that this set is also a subset of \mathcal{H}_N . Then, to repair the node of (41) that contains \mathbf{y}_1 (i.e., the one that corresponds to the first parity node of (37)) we download $\mathbf{X}_1 \mathbf{V}_a$ times the contents of the first parity in (41) and \mathbf{V}_a times the contents of the second parity. Hence, during this repair, the useful space is spanned by

$$[\mathbf{X}_1 \mathbf{V}_a \quad \mathbf{A}_1 \mathbf{V}_a] \quad (45)$$

and the interference space due to file part \mathbf{y}_s , $s \in \{2, \dots, k\}$, is

$$[\mathbf{X}_1 \mathbf{V}_a \quad (\mathbf{A}_s - \mathbf{A}_1) \mathbf{V}_a]. \quad (46)$$

Before we proceed, observe that the following hold

$$\mathcal{L}(\mathbf{X}_1 \mathbf{X}_s \mathbf{V}_a) = \mathcal{L}(\mathbf{V}_a) = \left\{ \left(\sum_{s=2}^{k+1} x_s \pmod{2} \right) \mathbf{e}_1 + \sum_{s=2}^{k+1} x_s \mathbf{e}_s; x_s \in \{0, 1\} \right\} \quad (47)$$

$$\Leftrightarrow \mathcal{L}(\mathbf{X}_1 \mathbf{V}_a) = \mathcal{L}(\mathbf{X}_s \mathbf{V}_a) = \left\{ \left(1 + \sum_{s=2}^{k+1} x_s \pmod{2} \right) \mathbf{e}_1 + \sum_{s=2}^{k+1} x_s \mathbf{e}_s; x_s \in \{0, 1\} \right\} \quad (48)$$

$$\Rightarrow \mathcal{L}(\mathbf{X}_{s_1} \mathbf{V}_a) = \mathcal{L}(\mathbf{X}_{s_2} \mathbf{V}_a), \quad (49)$$

for any $s, s_1, s_2 \in \{1, \dots, k+1\}$. The above equations imply that

$$\mathcal{L}(\mathbf{V}_a) \cup \mathcal{L}(\mathbf{X}_1 \mathbf{V}_a) = \left\{ \sum_{s=1}^{k+1} x_s; x_s \in \{0, 1\} \right\} = \mathcal{L}(\mathbf{H}_N). \quad (50)$$

Therefore, we have the following for each of the interference spaces

$$\begin{aligned} \frac{N}{2} &\leq \text{rank}([\mathbf{X}_1 \mathbf{V}_a \quad (a_s \mathbf{X}_s + (b_s - b_1) \mathbf{X}_{k+1} - a_1 \mathbf{X}_1) \mathbf{V}_a]) \\ &\leq |\mathcal{L}(\mathbf{X}_1 \mathbf{V}_a) \cup \mathcal{L}(\mathbf{X}_s \mathbf{V}_a) \cup \mathcal{L}(\mathbf{X}_{k+1} \mathbf{V}_a)| \\ &= |\mathcal{L}(\mathbf{X}_1 \mathbf{V}_a)| = \frac{N}{2}. \end{aligned} \quad (51)$$

Moreover, for the useful data space we have

$$\begin{aligned} \text{rank}([\mathbf{X}_1 \mathbf{V}_a \quad (a_1 \mathbf{X}_1 + b_1 \mathbf{X}_{k+1} + \mathbf{I}_N) \mathbf{V}_a]) &= \text{rank}([\mathbf{X}_1 \mathbf{V}_a \quad \mathbf{V}_a]) \\ &= |\mathcal{L}(\mathbf{V}_a) \cup \mathcal{L}(\mathbf{X}_1 \mathbf{V}_a)| = |\mathcal{L}(\mathbf{H}_N)| = N. \end{aligned} \quad (52)$$

Thus, we can perform optimal repair of the node containing \mathbf{y}_1 in (41), which is equivalent to optimally repairing the first parity of our code in (5).

B. Repairing the second parity

Here, we have an additional step. We first manipulate our coding matrices of (5) to obtain an equivalent representation for the same code. Then, in the same manner we rewrite this code in a form where the second parity of (5) is a systematic node in some representation. Without loss of generality, we can multiply any coding column block that multiplies the i th file part

$$\begin{bmatrix} \mathbf{I} \\ \mathbf{A}_i \end{bmatrix} = \begin{bmatrix} \mathbf{I} \\ a_i \mathbf{X}_i + b_i \mathbf{X}_{k+1} + \mathbf{I}_N \end{bmatrix} \quad (53)$$

with a full rank matrix and maintain the same code properties, as shown in [20]. In the following derivations, we use the fact that $\mathbf{X}_s^2 = \mathbf{I}_N$, for any $s \in \{1, \dots, k+1\}$. We multiply the i -th block of (5) with $a_i \mathbf{X}_i - b_i \mathbf{X}_{k+1} + \mathbf{I}_N$ to obtain

$$\begin{aligned} \begin{bmatrix} \mathbf{I}_N \\ a_i \mathbf{X}_i + b_i \mathbf{X}_{k+1} + \mathbf{I}_N \end{bmatrix} &\equiv \begin{bmatrix} a_i \mathbf{X}_i - b_i \mathbf{X}_{k+1} + \mathbf{I}_N \\ (a_i \mathbf{X}_i - b_i \mathbf{X}_{k+1} + \mathbf{I}_N)(a_i \mathbf{X}_i + b_i \mathbf{X}_{k+1} + \mathbf{I}_N) \end{bmatrix} = \begin{bmatrix} a_i \mathbf{X}_i - b_i \mathbf{X}_{k+1} + \mathbf{I}_N \\ (a_i \mathbf{X}_i + \mathbf{I}_N)^2 - b_i^2 \mathbf{I}_N \end{bmatrix} \\ &\equiv \begin{bmatrix} a_i \mathbf{X}_i - b_i \mathbf{X}_{k+1} + \mathbf{I}_N \\ 2a_i \mathbf{X}_i + (a_i^2 - b_i^2 + 1) \mathbf{I}_N \end{bmatrix} \stackrel{(*)}{=} \begin{bmatrix} a_i \mathbf{X}_i - b_i \mathbf{X}_{k+1} + \mathbf{I}_N \\ 2a_i \mathbf{X}_i \end{bmatrix}, \end{aligned} \quad (54)$$

where in (*) we use the fact that $a_i^2 - b_i^2 + 1 = 0$. We continue by multiplying the i -th column block with $(a_i)^{-1}\mathbf{X}_i$ to obtain

$$\begin{bmatrix} a_i\mathbf{X}_i - b_i\mathbf{X}_{k+1} + \mathbf{I}_N \\ 2a_i\mathbf{X}_i \end{bmatrix} \equiv \begin{bmatrix} \mathbf{I}_N - a_i^{-1}b_i\mathbf{X}_{k+1}\mathbf{X}_i + a_i^{-1}\mathbf{X}_i \\ 2\mathbf{I}_N \end{bmatrix} \equiv \begin{bmatrix} \mathbf{I}_N - a_i^{-1}b_i\mathbf{X}_{k+1}\mathbf{X}_i + a_i^{-1}\mathbf{X}_i \\ \mathbf{I}_N \end{bmatrix}, \quad (55)$$

where in the last step we multiplied the contents of the second parity with 2^{-1} . Hence, let

$$\mathbf{A}'_i = \mathbf{I}_N - a_i^{-1}b_i\mathbf{X}_{k+1}\mathbf{X}_i + a_i^{-1}\mathbf{X}_i, \quad i \in \{1, \dots, k\}. \quad (56)$$

Then, we rewrite our original code as

$$\begin{bmatrix} \mathbf{I}_N & \mathbf{0}_N & \dots & \mathbf{0}_N \\ \mathbf{0}_N & \mathbf{I}_N & \dots & \mathbf{0}_N \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0}_N & \mathbf{0}_N & \dots & \mathbf{I}_N \\ \mathbf{A}'_1 & \mathbf{A}'_2 & \dots & \mathbf{A}'_k \\ \mathbf{I}_N & \mathbf{I}_N & \dots & \mathbf{I}_N \end{bmatrix} \mathbf{f}' \quad (57)$$

where \mathbf{f}' is a full rank row transformation of \mathbf{f} . We proceed in the same manner that we handled the first parity repair. We make a change of variables such that the second parity becomes a systematic node in a new representation

$$\sum_{i=1}^k \mathbf{f}'_i = \mathbf{y}'_1 \quad (58)$$

and obtain the equivalent form

$$\begin{bmatrix} \mathbf{I}_N & -\mathbf{I}_N & \dots & -\mathbf{I}_N \\ \mathbf{0}_N & \mathbf{I}_N & \dots & \mathbf{0}_N \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0}_N & \mathbf{0}_N & \dots & \mathbf{I}_N \\ \mathbf{A}'_1 & \mathbf{A}'_2 - \mathbf{A}'_1 & \dots & \mathbf{A}'_k - \mathbf{A}'_1 \\ \mathbf{I}_N & \mathbf{0}_N & \dots & \mathbf{0}_N \end{bmatrix} \mathbf{y}', \quad (59)$$

where

$$\mathbf{A}'_1 = \mathbf{I}_N - a_1^{-1}b_1\mathbf{X}_{k+1}\mathbf{X}_1 + a_1^{-1}\mathbf{X}_1, \quad (60)$$

$$\mathbf{A}'_s - \mathbf{A}'_1 = a_s^{-1}\mathbf{X}_s - a_s^{-1}b_s\mathbf{X}_{k+1}\mathbf{X}_s + a_1^{-1}b_1\mathbf{X}_{k+1}\mathbf{X}_1 - a_1^{-1}\mathbf{X}_1 \quad (61)$$

Then, the parity node which corresponds to systematic node 1 here, can be repaired by using \mathbf{V}_b with columns in the set

$$\mathcal{V}_b = \left\{ \mathbf{X}_{k+1}^{x_{k+1}} \prod_{s=2}^k (\mathbf{X}_1 \mathbf{X}_s)^{x_s} \mathbf{w} : x_{k+1}, x_s \in \{0, 1\} \right\}. \quad (62)$$

Again, the following equations hold

$$\mathcal{L}(\mathbf{X}_{k+1} \mathbf{V}_b) = \mathcal{L}(\mathbf{V}_b) = \left\{ \left(\sum_{s=2}^k x_s \pmod{2} \right) \mathbf{e}_1 + \sum_{s=2}^{k+1} x_s \mathbf{e}_s; \quad x_s \in \{0, 1\} \right\}, \quad (63)$$

$$\mathcal{L}(\mathbf{X}_{s_1} \mathbf{V}_b) = \mathcal{L}(\mathbf{X}_{s_2} \mathbf{V}_b) = \left\{ \left(1 + \sum_{s=2}^k x_s \pmod{2} \right) \mathbf{e}_1 + \sum_{s=2}^{k+1} x_s \mathbf{e}_s; \quad x_s \in \{0, 1\} \right\}, \quad (64)$$

$$\text{and } \mathcal{L}(\mathbf{X}_{s_1} \mathbf{X}_{k+1} \mathbf{V}_b) = \mathcal{L}(\mathbf{X}_{s_1} \mathbf{V}_b), \quad (65)$$

for all $s_1, s_2 \in \{1, \dots, k\}$. Hence, we have for the interference space generated by component \mathbf{y}'_s , $s \in \{2, \dots, k\}$

$$\begin{aligned} \frac{N}{2} &\leq \text{rank}([\mathbf{X}_1 \mathbf{V}_b \quad (\mathbf{A}'_s - \mathbf{A}'_1) \mathbf{V}_b]) \\ &\leq |\mathcal{L}(\mathbf{X}_s \mathbf{V}_b) \cup \mathcal{L}(\mathbf{X}_1 \mathbf{V}_b) \cup \mathcal{L}(\mathbf{X}_{k+1} \mathbf{X}_1 \mathbf{V}_b) \cup \mathcal{L}(\mathbf{X}_{k+1} \mathbf{X}_s \mathbf{V}_b)| \\ &= |\mathcal{L}(\mathbf{X}_1 \mathbf{V}_b) \cup \mathcal{L}(\mathbf{X}_s \mathbf{V}_b)| = \frac{N}{2}. \end{aligned} \quad (66)$$

Moreover, the useful space is full rank

$$\text{rank}([\mathbf{X}_1 \mathbf{V}_b \quad (\mathbf{I}_N - a_1^{-1}b_1\mathbf{X}_{k+1}\mathbf{X}_1 + a_1^{-1}\mathbf{X}_1) \mathbf{V}_b]) = \text{rank}([\mathbf{X}_1 \mathbf{V}_b \quad \mathbf{V}_b]) = N. \quad (67)$$

Thus, we can perform optimal repair for the second parity of the code in (5), with repair bandwidth $(k+1)\frac{N}{2}$.

VII. THE MDS PROPERTY

In this section, we give explicit conditions on the a_i, b_i constants, for all $i \in \{1, \dots, k\}$, and the size of the finite field \mathbb{F}_q , for which the code in (5) is MDS. We discuss the MDS property using the notion of data collectors (DCs), in the same manner that it was used in [2]. A DC can be considered as an external user that can connect and has complete access to the contents of some subset of k nodes. A storage code where each node expends $\frac{M}{k}$ worth of storage, has the MDS property when all possible $\binom{n}{k}$ DCs can decode the file \mathbf{f} . We can show that testing the MDS property is equivalent to checking the rank of a specific matrix associated with each DC. This DC matrix is the vertical concatenation of the k stacks of equations stored by the nodes that the DC connects to. If all $\binom{n}{k}$ DC matrices are full rank, then we declare that the storage code has the MDS property.

We start with a DC that connects to systematic nodes $\{1, \dots, k-1\}$ and the first parity node. The determinant of the corresponding DC matrix is

$$\det \left(\left[\begin{array}{ccc|c} \mathbf{I}_N & \dots & \mathbf{0}_{N \times N} & \mathbf{0}_{N \times N} \\ \vdots & & \vdots & \vdots \\ \mathbf{0}_{N \times N} & \dots & \mathbf{I}_N & \mathbf{0}_{N \times N} \\ \hline \mathbf{I}_N & \dots & \mathbf{I}_N & \mathbf{I}_N \end{array} \right] \right) = \det(\mathbf{I}_N) \neq 0, \quad (68)$$

since \mathbf{I}_N is a full rank diagonal matrix. We continue by considering a DC that connects to systematic nodes $\{1, \dots, k-1\}$ and the second parity node. For that we have

$$\det \left(\left[\begin{array}{ccc|c} \mathbf{I}_N & \dots & \mathbf{0}_{N \times N} & \mathbf{0}_{N \times N} \\ \vdots & & \vdots & \vdots \\ \mathbf{0}_{N \times N} & \dots & \mathbf{I}_N & \mathbf{0}_{N \times N} \\ \hline \mathbf{A}_1 & \dots & \mathbf{A}_{k-1} & \mathbf{A}_k \end{array} \right] \right) = \det(\mathbf{A}_k) \neq 0, \quad (69)$$

due to \mathbf{A}_k being full rank.

Finally, we consider DCs that connect to k systematic nodes and both parity nodes. Let a DC that connects to systematic node $\{1, \dots, k-2\}$ and the two parities. The corresponding DC matrix is

$$\left[\begin{array}{ccc|cc} \mathbf{I}_N & \dots & \mathbf{0}_{N \times N} & \mathbf{0}_{N \times N} & \mathbf{0}_{N \times N} \\ \vdots & & \vdots & \vdots & \vdots \\ \mathbf{0}_{N \times N} & \dots & \mathbf{I}_N & \mathbf{0}_{N \times N} & \mathbf{0}_{N \times N} \\ \hline \mathbf{I}_N & \dots & \mathbf{I}_N & \mathbf{I}_N & \mathbf{I}_N \\ \mathbf{A}_1 & \dots & \mathbf{A}_{k-2} & \mathbf{A}_{k-1} & \mathbf{A}_k \end{array} \right]. \quad (70)$$

The leftmost $(k-2)N$ columns of the matrix in (70) are linearly independent, due to the upper-left identity block. Moreover, the leftmost $(k-2)N$ columns are linearly independent with the rightmost $2N$, using an analogous argument. Hence, we need to only check the rank of the sub-matrix

$$\begin{bmatrix} \mathbf{I}_N & \mathbf{I}_N \\ \mathbf{A}_{k-1} & \mathbf{A}_k \end{bmatrix}. \quad (71)$$

In the general case, a DC that connects to some $k-2$ subset of systematic nodes and the two parities has a corresponding matrix where the following block needs to be full rank so that the MDS property can be satisfied

$$\begin{bmatrix} \mathbf{I}_N & \mathbf{I}_N \\ \mathbf{A}_i & \mathbf{A}_j \end{bmatrix}, \quad (72)$$

for $i, j \in \{1, \dots, k\}$ and $i \neq j$. The code is MDS when

$$\begin{aligned} & \text{rank} \left(\begin{bmatrix} \mathbf{I}_N & \mathbf{I}_N \\ a_i \mathbf{X}_i + b_i \mathbf{X}_{k+1} + \mathbf{I}_N & a_j \mathbf{X}_j + b_j \mathbf{X}_{k+1} + \mathbf{I}_N \end{bmatrix} \right) \\ &= \text{rank} \left(\begin{bmatrix} \mathbf{I}_N & \mathbf{I}_N \\ a_i \mathbf{X}_i + b_i \mathbf{X}_{k+1} + \mathbf{I}_N & a_j \mathbf{X}_j + b_j \mathbf{X}_{k+1} + \mathbf{I}_N \end{bmatrix} \times \begin{bmatrix} \mathbf{I}_N & \mathbf{I}_N \\ \mathbf{0}_{N \times N} & -\mathbf{I}_N \end{bmatrix} \right) \\ &= \text{rank} \left(\begin{bmatrix} \mathbf{I}_N & 0 \\ a_i \mathbf{X}_i + b_i \mathbf{X}_{k+1} + \mathbf{I}_N & a_i \mathbf{X}_i - a_j \mathbf{X}_j + (b_i - b_j) \mathbf{X}_{k+1} \end{bmatrix} \right) \\ &= \frac{N}{2} + \text{rank}(a_i \mathbf{X}_i - a_j \mathbf{X}_j + (b_i - b_j) \mathbf{X}_{k+1}) = N, \end{aligned} \quad (73)$$

for all $i, j \in \{1, \dots, k\}$, which is true if

$$\text{rank}(a_i \mathbf{X}_i - a_j \mathbf{X}_j + (b_i - b_j) \mathbf{X}_{k+1}) = \frac{N}{2}. \quad (74)$$

Since the diagonal elements of \mathbf{X}_i are $\{\pm 1\}$, the previous requirement gives the lemma.

Lemma 3: The code in (5) is MDS when

$$i) \ a_i - a_j + (b_i - b_j) \neq 0, \quad (75)$$

$$ii) \ a_i + a_j - (b_i - b_j) \neq 0, \quad (76)$$

$$iii) \ a_i - a_j - (b_i - b_j) \neq 0, \quad (77)$$

$$\text{and } iv) \ a_i + a_j + (b_i - b_j) \neq 0, \quad (78)$$

for all $i \neq j \in \{1, \dots, k\}$.

Now, remember that our initial constraint on the a_i and b_i constants was

$$a_i^2 - b_i^2 = -1 \Leftrightarrow (a_i - b_i)(a_i + b_i) = -1. \quad (79)$$

one solution to the previous equation is the following

$$a_i - b_i = x_i \quad (80)$$

$$a_i + b_i = -x_i^{-1}, \quad (81)$$

If we input the above solution to (79), then the MDS equations (75)-(78) become

$$\begin{aligned} a_i - a_j + (b_i - b_j) &= a_i + b_i - (a_i + b_j) \\ &= -x_i^{-1} + x_j^{-1} \neq 0 \\ &\Leftrightarrow x_i^{-1} \neq x_j^{-1}, \end{aligned} \quad (82)$$

$$\begin{aligned} a_i + a_j - (b_i - b_j) &= a_i - b_i + a_j + b_j \\ &= x_i - x_j^{-1} \neq 0 \\ &\Leftrightarrow x_i \neq x_j^{-1}, \end{aligned} \quad (83)$$

$$\begin{aligned} a_i - a_j - (b_i - b_j) &= a_i - b_i - (a_j - b_j) \\ &= x_i - x_j \neq 0 \\ &\Leftrightarrow x_i \neq x_j, \end{aligned} \quad (84)$$

$$\begin{aligned} a_i + a_j + (b_i - b_j) &= a_i + b_i + a_j - b_j \\ &= -x_i^{-1} + x_j \neq 0 \\ &\Leftrightarrow x_i^{-1} \neq x_j, \end{aligned} \quad (85)$$

The above conditions can be equivalently stated as

$$x_i \neq x_j \text{ and } x_i x_j \neq 1, \quad (86)$$

for any $i \neq j \in \{1, \dots, k\}$.

Then, consider a prime field \mathbb{F}_q of size q . The set of x_i s that satisfies our MDS requirements, is such in which no two elements are inverses of each other. It is known that, over a prime field, half the nonzero elements are inverses of the other nonzero half. If we additionally do not consider $x_i \in \{1, q-1\}$, then we are left with $\frac{q-3}{2}$ elements. Therefore, we can consider a prime field of size q that has the property

$$k \leq \frac{q-3}{2} \Leftrightarrow q \geq 2k+3 \quad (87)$$

and obtain x_1, \dots, x_k such that our requirements are satisfied. Then, the elements a_i and b_i , for all $i \in \{1, \dots, k\}$, can be obtained through the following equations

$$a_i = 2^{-1}x_i - 2^{-1}x_i^{-1} \quad (88)$$

$$b_i = -2^{-1}x_i - 2^{-1}x_i^{-1}. \quad (89)$$

Observe that the above solutions yield $a_i \neq 0$ (that is needed for successful repair), for all $i \in \{1, \dots, k\}$, when $x_i \notin \{0, 1, q-1\}$. Therefore a prime field of size greater than, or equal to $2k+3$ always suffices to obtain the MDS property.

VIII. GENERALIZING TO MORE THAN 2 PARITIES

A. m -parity codes with optimal systematic repair

We generalize the Hadamard design construction of Section III and of the code in [26], to construct $(k+m, k)$ MDS storage codes for file sizes $M = km^k$. Our constructions are based on a generalization of the Sylvester construction for complex Hadamard matrices that use m^{th} roots of unity. We generate these matrices as

$$\mathbf{H}_{m^k} = \mathbf{H}_m \otimes \mathbf{H}_{m^{k-1}}, \quad (90)$$

where \mathbf{H}_m is the m -point Discrete Fourier Transform matrix over a finite field. For example, for $m = 3$ and \mathbb{F}_7 , we have

$$\mathbf{H}_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \rho & \rho^2 \\ 1 & \rho^2 & \rho \end{bmatrix} \text{ and } \mathbf{H}_9 = \begin{bmatrix} \mathbf{H}_3 & \mathbf{H}_3 & \mathbf{H}_3 \\ \mathbf{H}_3 & \rho \mathbf{H}_3 & \rho^2 \mathbf{H}_3 \\ \mathbf{H}_3 & \rho^2 \mathbf{H}_3 & \rho \mathbf{H}_3 \end{bmatrix}, \quad (91)$$

where $\rho = 2$. Then, we consider the set

$$\mathcal{H}_{m^k} = \left\{ \prod_{i=1}^k \mathbf{X}_i^{x_i} \mathbf{w} : x_i \in \{0, 1, \dots, m-1\} \right\}, \quad (92)$$

where $\mathbf{w} = \mathbf{1}_{m^k \times 1}$ and

$$\mathbf{X}_i = \mathbf{I}_{m^{i-1}} \otimes \text{blkdiag} \left(\mathbf{I}_{\frac{N}{m^i}}, \rho \mathbf{I}_{\frac{N}{m^i}}, \dots, \rho^{m-1} \mathbf{I}_{\frac{N}{m^i}} \right). \quad (93)$$

Here, ρ denotes an m^{th} root of unity which yields

$$\mathbf{X}_i^m = \mathbf{I}_{m^k}. \quad (94)$$

As with the $m = 2$ case, there is a one-to-one correspondence between the elements of the set \mathcal{H}_{m^k} and the columns of \mathbf{H}_{m^k} . The general m proof for that property follows the same manner of the $m = 2$ case, thus we omit it.

Remark 5: To maintain the full rank property of \mathbf{H}_{m^k} , the finite field over which we operate should be chosen such that all m^{th} roots of unity are distinct. The number of distinct m^{th} roots of unity over a finite field \mathbb{F}_q is given by the number of (distinct) solutions of the equation $x^m = 1$. This is equal to the order of the cyclic group that generates m^{th} roots of unity within the multiplicative group of \mathbb{F}_q . This subgroup has order m when m divides $q-1$ [27].

1) *Code construction:* Our $(k+m, k)$ MDS code encodes a file \mathbf{f} of size $M = km^k$ in the manner of

$$\begin{bmatrix} \mathbf{I}_{km^k} \\ \mathbf{A}^{(k,m)} \end{bmatrix} \mathbf{f}, \quad (95)$$

where

$$\mathbf{A}^{(k,m)} = \begin{bmatrix} \mathbf{I}_{m^k} & \mathbf{I}_{m^k} & \dots & \mathbf{I}_{m^k} \\ \lambda_{1,1} \mathbf{X}_1 & \lambda_{1,2} \mathbf{X}_2 & \dots & \lambda_{1,k} \mathbf{X}_k \\ \lambda_{2,1} \mathbf{X}_1^2 & \lambda_{2,2} \mathbf{X}_2^2 & \dots & \lambda_{2,k} \mathbf{X}_k^2 \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{m-1,k} \mathbf{X}_1^{m-1} & \lambda_{m-1,2} \mathbf{X}_2^{m-1} & \dots & \lambda_{m-1,k} \mathbf{X}_k^{m-1} \end{bmatrix}, \quad (96)$$

with $\lambda_{i,j} \in \mathbb{F}_q$.

2) *Optimal repair of the systematic nodes:* For this code, let systematic node $i \in \{1, \dots, k\}$ fail. Then, to repair it we construct the repair matrix \mathbf{V}_i that has as columns the elements of set

$$\mathcal{V}_i = \left\{ \prod_{s=1, s \neq i}^k \mathbf{X}_s^{x_s} \mathbf{w} : x_s \in \{0, 1, \dots, m-1\} \right\}. \quad (97)$$

This matrix is used to multiply the contents of each of the parity nodes. Here, the useful space during the repair is given by

$$[\mathbf{V}_i \quad \mathbf{X}_i \mathbf{V}_i \quad \mathbf{X}_i^2 \mathbf{V}_i \quad \dots \quad \mathbf{X}_i^{m-1} \mathbf{V}_i] \quad (98)$$

and the interference space generated by systematic component $j \neq i$ is spanned by

$$[\mathbf{V}_i \quad \mathbf{X}_j \mathbf{V}_i \quad \mathbf{X}_j^2 \mathbf{V}_i \quad \dots \quad \mathbf{X}_j^{m-1} \mathbf{V}_i]. \quad (99)$$

Due to the modulus- m property of the powers of the \mathbf{X}_i matrices, we obtain the following under the lattice representation

$$\mathcal{L}(\mathbf{V}_i) = \mathcal{L}(\mathbf{X}_j^{l_1} \mathbf{V}_i) \text{ and } \mathcal{L}(\mathbf{X}_i^{l_1} \mathbf{V}_i) \cap \mathcal{L}(\mathbf{X}_i^{l_2} \mathbf{V}_i) = \emptyset, \quad (100)$$

for any $j \in \{1, \dots, k\} \neq i$, and $l, l_1, l_2 \in \{0, \dots, m-1\}$, with $l_1 \neq l_2$. The above property and the fact that the elements of \mathcal{H}_{m^k} are linearly independent leads us to the following lemma.

Lemma 4: For any $i, j \in \{1, 2, \dots, k\}$ we have that

$$\text{rank}([\mathbf{V}_i \quad \mathbf{X}_j \mathbf{V}_i \quad \mathbf{X}_j^2 \mathbf{V}_i \quad \dots \quad \mathbf{X}_j^{m-1} \mathbf{V}_i]) = |\mathcal{L}(\mathbf{V}_i) \cup \mathcal{L}(\mathbf{X}_j \mathbf{V}_i) \cup \mathcal{L}(\mathbf{X}_j^2 \mathbf{V}_i) \cup \dots \cup \mathcal{L}(\mathbf{X}_j^{m-1} \mathbf{V}_i)| \quad (101)$$

$$= \begin{cases} m^k, & i = j, \\ m^{k-1}, & i \neq j. \end{cases} \quad (102)$$

By Lemma (4) we see that each of the $k-1$ interference terms is confined within m^{k-1} dimensions and the full rank property of the useful space is maintained. This is equivalent to stating that we can repair a single systematic node failure by downloading exactly $m^k + (k-1)m^{k-1} = (n-1)m^{k-1}$ equations, which matches exactly the information theoretic repair optimal of [2].

In Fig. 9 we give an illustration of the repair spaces for a $(6, 3)$ code. We sketch the structure of our code on the left of the figure. Each parity block is associated with a specific key matrix \mathbf{X}_i . This allows a selection of \mathbf{V}_i that is an invariant subspace to all matrices but to the key, one which multiplies the desired and lost file piece. This selection of \mathbf{V}_i results in perfect alignment of interference in 3^2 dimensions, while ensuring a full rank 3^3 useful space.

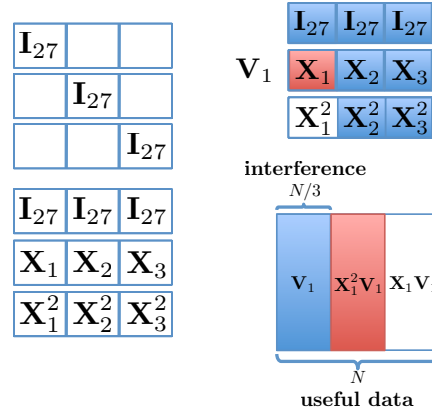


Fig. 9. A $(6, 3)$ systematic-repair optimal code.

3) *Suboptimal repair of the parities:* In contrast to our 2-parity code of (5), for this m -parity code, a parity node failure is repaired using the scheme of Wu *et al.* [12]. We first rewrite our code in a new systematic re-interpretation, where the lost parity is now in systematic form, in the same manner of the parity repair of our 2-parity code. During the repair, we align a single interference block by inverting the corresponding matrices. This induces a repair download of $m^{k-1} + (n-2)m^k$ equations, which suffices to exactly reconstruct what was lost. This repair strategy is only optimal for $(n, 2)$ codes and asymptotically matches the file size for large k .

4) *The MDS property:* We establish the MDS property of our m -parity codes in a probabilistic sense: we show that when we select the $\lambda_{i,j}$ variables uniformly at random over a sufficiently large finite field, then the code is MDS with probability arbitrarily close to 1. This is shown using the Schwartz-Zippel lemma [29], [30] on a nonzero polynomial on $\lambda_{i,j}$ s induced by the products of all possible DC matrix determinants.

Let a DC of the code in (95) that connects to $k-p$ systematic nodes and p parities. For simplicity consider that this is the DC that is connected to the last $k-p$ systematic nodes and the first p parity nodes. The induced determinant of the corresponding DC matrix will be zero if the following determinant is zero

$$\det \left(\begin{bmatrix} \mathbf{I}_{m^k} & \mathbf{I}_{m^k} & \dots & \mathbf{I}_{m^k} \\ \lambda_{1,1} \mathbf{X}_1 & \lambda_{1,2} \mathbf{X}_2 & \dots & \lambda_{1,k} \mathbf{X}_k \\ \lambda_{2,1} \mathbf{X}_1^2 & \lambda_{2,2} \mathbf{X}_2^2 & \dots & \lambda_{2,k} \mathbf{X}_k^2 \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{p-1,1} \mathbf{X}_1^{p-1} & \lambda_{p-1,2} \mathbf{X}_2^{p-1} & \dots & \lambda_{p-1,k} \mathbf{X}_k^{p-1} \end{bmatrix} \right) = |\mathbf{I}_{(k-p)m^k}| \det \left(\begin{bmatrix} \mathbf{I}_{m^k} & \mathbf{I}_{m^k} & \dots & \mathbf{I}_{m^k} \\ \lambda_{1,1} \mathbf{X}_1 & \lambda_{1,2} \mathbf{X}_2 & \dots & \lambda_p^{(1)} \mathbf{X}_p \\ \lambda_{2,1} \mathbf{X}_1^2 & \lambda_{2,2} \mathbf{X}_2^2 & \dots & \lambda_p^{(2)} \mathbf{X}_p^2 \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{p-1,1} \mathbf{X}_1^{p-1} & \lambda_{p-1,2} \mathbf{X}_2^{p-1} & \dots & \lambda_{p-1,p} \mathbf{X}_p^{p-1} \end{bmatrix} \right). \quad (103)$$

Since each of the \mathbf{X}_i matrices is diagonal, each column of the matrix in the right hand side of (103) has exactly p nonzero elements. These, pm^k columns can be considered to fall into m^k groups, with each element of a group having identical non-zero support with any other vector in that group. Then, any two columns within a block

$$\begin{bmatrix} \mathbf{I}_{m^k} \\ \lambda_{1,i} \mathbf{X}_i \\ \lambda_{2,i} \mathbf{X}_i^2 \\ \vdots \\ \lambda_{p-1,i} \mathbf{X}_i^{p-1} \end{bmatrix} \quad (104)$$

are orthogonal since their nonzero supports have zero overlap. Hence, a linear dependence will only exist among columns of a given non-zero support. We can then rewrite the matrix determinant of (103) as

$$\det \left(\mathbf{P}_r \begin{bmatrix} \mathbf{B}_1 & \mathbf{0}_{m^k \times m^k} & \cdots & \mathbf{0}_{m^k \times m^k} \\ \mathbf{0}_{m^k \times m^k} & \mathbf{B}_2 & \cdots & \mathbf{0}_{m^k \times m^k} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0}_{m^k \times m^k} & \cdots & \mathbf{0}_{m^k \times m^k} & \mathbf{B}_p \end{bmatrix} \mathbf{P}_c \right) = |\mathbf{P}_r| |\mathbf{P}_c| \prod_{i=1}^{m^k} |\mathbf{B}_i| \quad (105)$$

where \mathbf{P}_r and \mathbf{P}_c are the permutation matrices that group the columns and rows of the matrix according to their non-zero support so to generate the block diagonal matrix. The $p \times p$ matrix \mathbf{B}_i is of the form

$$\begin{bmatrix} \rho_{i1,j1} \lambda_{i1,j1} & \rho_{i1,j2} \lambda_{i1,j2} & \cdots & \rho_{i1,jp} \lambda_{i1,jp} \\ \rho_{i2,j1} \lambda_{i2,j1} & \rho_{i2,j2} \lambda_{i2,j2} & \cdots & \rho_{i2,jp} \lambda_{i2,jp} \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{ip,j1} \lambda_{ip,j1} & \rho_{ip,j2} \lambda_{ip,j2} & \cdots & \rho_{ip,jp} \lambda_{ip,jp} \end{bmatrix}. \quad (106)$$

where $\rho_{i1,j1}$ is some m^{th} root of unity, the indices depend on i , and no $\lambda_{i,j}$ appears more than once within each matrix. We can expand the determinant of any \mathbf{B}_i matrix using the Leibniz formula, where $p!$ monomials of degree p appear. Each one of them includes a different subset of the $\lambda_{i,j}$ variables. Hence, the induced polynomial cannot be the zero polynomial. Therefore, the determinant of \mathbf{B}_i is a nonzero polynomial of degree p in the $\lambda_{i,j}$ variables, hence $\prod_{i=1}^{m^k} |\mathbf{B}_i|$ is also a non zero polynomial of degree pm^k in the $\lambda_{i,j}$ variables. Accordingly, we can compute the determinant of each DC in this way. In the same manner, each of them will be a nonzero polynomial in $\lambda_{i,j}$. The product of all these determinants be a nonzero polynomial in $\lambda_{i,j}$ of some degree d . By the Schwartz-Zippel lemma [30], we know that when we draw $\lambda_{i,j}$ uniformly at random over a field of size q , this induced polynomial is zero with probability less than or equal to $\frac{d}{q}$. Hence, the MDS property is satisfied with probability arbitrarily close to 1, for sufficiently large finite fields.

IX. CONNECTION TO PERMUTATION-MATRIX BASED CODES

Here we investigate some interesting connections between our systematic-repair optimal codes of Section VIII and the permutation-matrix based codes presented in [21] and [23]. Under a similarity transformation, our codes are equivalent to ones with coding matrices picked as specific permutation matrices. Multiplying the column space of an \mathbf{X}_i matrix of our construction with the Hadamard matrix \mathbf{H}_{m^k} , yields a matrix that is a permutation of the columns of the Hadamard matrix

$$\mathbf{H}_{m^k}^{-1} \mathbf{X}_i \mathbf{H}_{m^k} = \mathbf{H}_{m^k}^{-1} \mathbf{H}_{m^k} \mathbf{P}_i = \mathbf{P}_i, \quad (107)$$

where \mathbf{P}_i is some permutation matrix. This is due to the fact that the elements of \mathcal{H}_{m^k} wrap around, i.e., $\mathcal{L}(\mathbf{H}_{m^k}) = \mathcal{L}(\mathbf{X}_i \mathbf{H}_{m^k})$ for any i .

Example Consider the $m = 2, k = 3$ case:

$$\mathbf{H}_{2^3} = [\mathbf{w} \quad \mathbf{X}_2 \mathbf{w} \quad \mathbf{X}_1 \mathbf{w} \quad \mathbf{X}_1 \mathbf{X}_2 \mathbf{w}] \quad (108)$$

$$\mathbf{X}_1 \mathbf{H}_{2^3} = [\mathbf{X}_1 \mathbf{w} \quad \mathbf{X}_1 \mathbf{X}_2 \mathbf{w} \quad \mathbf{w} \quad \mathbf{X}_2 \mathbf{w}] = \mathbf{H}_{2^3} \mathbf{P}_1 \quad (109)$$

$$\mathbf{X}_2 \mathbf{H}_{2^3} = [\mathbf{X}_2 \mathbf{w} \quad \mathbf{w} \quad \mathbf{X}_1 \mathbf{X}_2 \mathbf{w} \quad \mathbf{X}_1 \mathbf{w}] = \mathbf{H}_{2^3} \mathbf{P}_2, \quad (110)$$

where \mathbf{P}_1 and \mathbf{P}_2 are permutation matrices. The wrap-round property of the columns of the Hadamard matrix produces permutations of itself when multiplied by the \mathbf{X}_i matrices, and each permutation is distinct.

Without loss of generality [16], we can rewrite the $\mathbf{A}^{(m,k)}$ matrix of (95) as

$$\begin{aligned} \mathbf{H}_{m^k}^{-1} \mathbf{A}^{(k,m)} (\mathbf{I}_k \otimes \mathbf{H}_{m^k}) &= \mathbf{H}_{m^k}^{-1} \begin{bmatrix} \mathbf{I}_{m^k} \mathbf{H}_{m^k} & \mathbf{I}_{m^k} \mathbf{H}_{m^k} & \cdots & \mathbf{I}_{m^k} \mathbf{H}_{m^k} \\ \lambda_{1,1} \mathbf{X}_1 \mathbf{H}_{m^k} & \lambda_{1,2} \mathbf{X}_2 \mathbf{H}_{m^k} & \cdots & \lambda_{1,k} \mathbf{X}_k \mathbf{H}_{m^k} \\ \lambda_{2,1} \mathbf{X}_1^2 \mathbf{H}_{m^k} & \lambda_{2,2} \mathbf{X}_2^2 \mathbf{H}_{m^k} & \cdots & \lambda_{2,k} \mathbf{X}_k^2 \mathbf{H}_{m^k} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{m-1,k} \mathbf{X}_1^{m-1} \mathbf{H}_{m^k} & \lambda_{m-1,2} \mathbf{X}_2^{m-1} \mathbf{H}_{m^k} & \cdots & \lambda_{m-1,k} \mathbf{X}_k^{m-1} \mathbf{H}_{m^k} \end{bmatrix} \\ &= \mathbf{H}_{m^k}^{-1} \begin{bmatrix} \mathbf{H}_{m^k} & \mathbf{H}_{m^k} & \cdots & \mathbf{H}_{m^k} \\ \lambda_{1,1} \mathbf{H}_{m^k} \mathbf{P}_{1,1} & \lambda_{1,2} \mathbf{H}_{m^k} \mathbf{P}_{1,2} & \cdots & \lambda_{1,k} \mathbf{H}_{m^k} \mathbf{P}_{1,k} \\ \lambda_{2,1} \mathbf{H}_{m^k} \mathbf{P}_{2,1} & \lambda_{2,2} \mathbf{H}_{m^k} \mathbf{P}_{2,2} & \cdots & \lambda_{2,k} \mathbf{H}_{m^k} \mathbf{P}_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{m-1,k} \mathbf{H}_{m^k} \mathbf{P}_{m-1,1} & \lambda_{m-1,2} \mathbf{H}_{m^k} \mathbf{P}_{m-1,2} & \cdots & \lambda_{m-1,k} \mathbf{H}_{m^k} \mathbf{P}_{m-1,k} \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{I}_{m^k} & \mathbf{I}_{m^k} & \cdots & \mathbf{I}_{m^k} \\ \lambda_{1,1} \mathbf{P}_{1,1} & \lambda_{1,2} \mathbf{P}_{1,2} & \cdots & \lambda_{1,k} \mathbf{P}_{1,k} \\ \lambda_{2,1} \mathbf{P}_{2,1} & \lambda_{2,2} \mathbf{P}_{2,2} & \cdots & \lambda_{2,k} \mathbf{P}_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{m-1,k} \mathbf{P}_{m-1,1} & \lambda_{m-1,2} \mathbf{P}_{m-1,2} & \cdots & \lambda_{m-1,k} \mathbf{P}_{m-1,k} \end{bmatrix}, \quad (111) \end{aligned}$$

where $\mathbf{P}_{i,j}$ is a permutation matrix. The systematic nodes of this equivalent $(k+m, m)$ MDS code can be optimally repaired using the repair matrices $\mathbf{V}_i \mathbf{H}_i^{-1}$, where \mathbf{V}_i has the columns of the set $\mathcal{V}_i = \left\{ \prod_{s=1, s \neq i}^k \mathbf{X}_s^{x_s} \mathbf{w} : x_s \in \{0, 1, \dots, m-1\} \right\}$. This is true since the rank properties of the corresponding useful and interference spaces remain the same under full rank column transformations. Interestingly, this connection is two-way. We give an example of a permutation code from [23] that exactly maps to our designs.

Example We consider the $(5, 3)$ permutation code of [23], designed for file sizes $M = 3 \cdot 2^3$. The three coding matrices of the first parity of this code are three identity matrices \mathbf{I}_8 . The three coding matrices of the second parity are three permutation matrices

$$\mathbf{P}_1 = \mathbf{I}_{\{5,6,7,8,1,2,3,4\},:}, \quad \mathbf{P}_2 = \mathbf{I}_{\{3,4,1,2,7,8,5,6\},:}, \quad \text{and} \quad \mathbf{P}_3 = \mathbf{I}_{\{2,1,4,3,6,5,8,7\},:}, \quad (112)$$

where $\mathbf{I}_{\{i_1, i_2, i_3, i_4, i_5, i_6, i_7, i_8\},:}$ indicates a permutation of the columns of the 8×8 identity matrix. We know that these matrices commute, therefore since they are normal, they can be simultaneously diagonalized under a common eigen basis. It can be checked that a common basis for the above commuting permutation matrices is the Hadamard matrix, which gives

$$\mathbf{H}_8 \mathbf{P}_1 \mathbf{H}_8^T = \mathbf{X}_1, \quad \mathbf{H}_8 \mathbf{P}_2 \mathbf{H}_8^T = \mathbf{X}_2, \quad \mathbf{H}_8 \mathbf{P}_3 \mathbf{H}_8^T = \mathbf{X}_3. \quad (113)$$

The connection manifested by the above equivalence examples seems very interesting. We believe that further investigation on it can lead to better understanding of the repair optimal high-rate MDS code regime.

X. CONCLUSIONS

We presented the first explicit, high-rate, $(k+2, k)$ erasure MDS storage code that achieves optimal repair bandwidth for any single node failure, including the parities. Our construction is based on perfect interference alignment properties offered by Hadamard designs. We generalize our 2-parity constructions to erasure codes with m -parities that achieve optimal repair of the systematic parts.

XI. ACKNOWLEDGEMENT

The authors would like to thank Changho Suh for insightful discussions.

APPENDIX

Proof of Lemma 1: Observe that $\mathbf{H}_N = \mathbf{H}_N^T$ and

$$\begin{aligned} \mathbf{H}_N \mathbf{H}_N^T &= \mathbf{H}_N \mathbf{H}_N = \begin{bmatrix} 2\mathbf{H}_{\frac{N}{2}} \mathbf{H}_{\frac{N}{2}} & \mathbf{0}_{\frac{N}{2} \times \frac{N}{2}} \\ \mathbf{0}_{\frac{N}{2} \times \frac{N}{2}} & 2\mathbf{H}_{\frac{N}{2}} \mathbf{H}_{\frac{N}{2}} \end{bmatrix} = 2 \left(\mathbf{I}_2 \otimes \mathbf{H}_{\frac{N}{2}} \mathbf{H}_{\frac{N}{2}} \right) \\ &= 2 \left(\mathbf{I}_2 \otimes 2 \left(\mathbf{I}_2 \otimes \mathbf{H}_{\frac{N}{2}} \mathbf{H}_{\frac{N}{4}} \right) \right) \\ &= 4 \left(\mathbf{I}_4 \otimes \mathbf{H}_{\frac{N}{4}} \mathbf{H}_{\frac{N}{4}} \right) \\ &\vdots \\ &= N \cdot (\mathbf{I}_N \otimes \mathbf{H}_1 \mathbf{H}_1) = N \cdot \mathbf{I}_N. \end{aligned} \quad (114)$$

We also have that $N \not\equiv 0 \pmod{q}$, for $q > 2$, thus the rank of \mathbf{H}_N is N and its columns are mutually orthogonal. \square

Then, let an $N \times N$ diagonal matrix

$$\mathbf{X}_i = \mathbf{I}_{2^{i-1}} \otimes \text{blkdiag} \left(\mathbf{I}_{\frac{N}{2^i}}, -\mathbf{I}_{\frac{N}{2^i}} \right) \quad (115)$$

defined for $i = \{1, \dots, \log_2(N)\}$. \mathbf{X}_i is a diagonal matrix, whose elements is a series of alternating 1s and -1 s, starting with $\frac{N}{2^i}$ 1s that flip to -1 s and back every $\frac{N}{2^i}$ positions. We can now expand \mathbf{H}_N in the following way

$$\mathbf{H}_N = \begin{bmatrix} \mathbf{H}_{\frac{N}{2}} & \mathbf{H}_{\frac{N}{2}} \\ \mathbf{H}_{\frac{N}{2}} & -\mathbf{H}_{\frac{N}{2}} \end{bmatrix} = \begin{bmatrix} \underbrace{\mathbf{1}_{2 \times 1} \otimes \mathbf{H}_{\frac{N}{2}}}_{\mathbf{F}_1} & \mathbf{X}_1 \left(\mathbf{1}_{2 \times 1} \otimes \mathbf{H}_{\frac{N}{2}} \right) \end{bmatrix}. \quad (116)$$

We proceed in the same manner by expanding all “smaller” $\mathbf{H}_{\frac{N}{2^i}}$ s

$$\begin{aligned} \mathbf{F}_1 &= \mathbf{1}_{2 \times 1} \otimes \left[\mathbf{1}_{2 \times 1} \otimes \mathbf{H}_{\frac{N}{2^2}} \quad \mathbf{X}_1 \left(\mathbf{1}_{2 \times 1} \otimes \mathbf{H}_{\frac{N}{2^2}} \right) \right] = \left[\underbrace{\mathbf{1}_{2^2 \times 1} \otimes \mathbf{H}_{\frac{N}{2^2}}}_{\mathbf{F}_2} \quad \mathbf{X}_2 \left(\mathbf{1}_{2^2 \times 1} \otimes \mathbf{H}_{\frac{N}{2^2}} \right) \right] \\ \mathbf{F}_2 &= \left[\underbrace{\mathbf{1}_{2^3 \times 1} \otimes \mathbf{H}_{\frac{N}{2^3}}}_{\mathbf{F}_3} \quad \mathbf{X}_3 \left(\mathbf{1}_{2^3 \times 1} \otimes \mathbf{H}_{\frac{N}{2^3}} \right) \right] \\ &\vdots \\ \mathbf{F}_{\log_2(N)-1} &= \left[\mathbf{1}_{N \times 1} \quad \mathbf{X}_{\log_2(N)} \mathbf{1}_{N \times 1} \right], \end{aligned} \quad (117)$$

where \mathbf{F}_i is an $N \times \frac{N}{2^i}$ matrix. Thus,

$$\begin{aligned} \text{span}(\mathbf{H}_N) &= \text{span}([\mathbf{F}_1 \quad \mathbf{X}_1 \mathbf{F}_1]) = \text{span}([\mathbf{F}_2 \quad \mathbf{X}_2 \mathbf{F}_2 \quad \mathbf{X}_1 \mathbf{F}_2 \quad \mathbf{X}_1 \mathbf{X}_2 \mathbf{F}_2]) \\ &\vdots \\ &= \text{span} \left(\left\{ \prod_{i=1}^{\log_2(N)} \mathbf{X}_i^{x_i} \mathbf{w} : x_i \in \{0, 1\} \right\} \right), \end{aligned} \quad (118)$$

which proves the final part of Lemma 1. \square

REFERENCES

- [1] The Coding for Distributed Storage wiki <http://tinyurl.com/storagecoding>
- [2] A. G. Dimakis, P. G. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, “Network coding for distributed storage systems,” in *IEEE Trans. on Inform. Theory*, vol. 56, pp. 4539 – 4551, Sep. 2010.
- [3] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, “A survey on network codes for distributed storage,” in *IEEE Proceedings*, vol. 99, pp. 476 – 489, Mar. 2011.
- [4] S. Ghemawat, H. Gobioff, and S.-T. Leung, “The Google file system,” in *Proc. ACM Symp. on Op. Sys. Principles (SOSP)*, Oct., 2003.
- [5] O. Khan, R. Burns, J. Plank, and C. Huang, “In search of I/O-optimal recovery from disk failures,” to appear in *Hot Storage 2011, 3rd Workshop on Hot Topics in Storage and File Systems*, Portland, OR, Jun., 2011.
- [6] H. Weatherspoon and J. D. Kubiatowicz, “Erasure coding vs. replication: a quantitative comparison,” in *Proc. IPTPS*, 2002.
- [7] M. Blaum, J. Brady, J. Bruck, and J. Menon, “EVENODD: An efficient scheme for tolerating double disk failures in raid architectures,” in *IEEE Transactions on Computers*, 1995.
- [8] Z. Wang, A. G. Dimakis, and J. Bruck, “Rebuilding for array codes in distributed storage systems,” in *Proc. Workshop on the Application of Communication Theory to Emerging Memory Technologies (ACTEMT)*, 2010.
- [9] L. Xiang, Y. Xu, J.C.S. Lui, and Q. Chang, “Optimal recovery of single disk failure in RDP code storage systems” in *Proc. ACM SIGMETRICS (2010) international conference on Measurement and modeling of computer systems*
- [10] F. Oggier and A. Datta, “Self-repairing homomorphic codes for distributed storage systems,” in *Proc. IEEE Infocom 2011*, Shanghai, China, Apr. 2011.
- [11] V. R. Cadambe and S. A. Jafar, “Interference alignment and the degrees of freedom for the K user interference channel,” *IEEE Trans. on Inform. Theory*, vol. 54, pp. 3425–3441, Aug. 2008.
- [12] Y. Wu and A. G. Dimakis, “Reducing repair traffic for erasure coding-based storage via interference alignment,” in *Proc. IEEE Int. Symp. on Information Theory (ISIT)*, Seoul, Korea, Jul. 2009.
- [13] K.V. Rashmi, N. B. Shah, P. V. Kumar, and K. Ramchandran, “Exact regenerating codes for distributed storage,” in *Allerton Conf. on Control, Comp., and Comm.*, Urbana-Champaign, IL, September 2009.
- [14] N. B. Shah, K. V. Rashmi, P. V. Kumar, and K. Ramchandran, “Explicit codes minimizing repair bandwidth for distributed storage,” in *Proc. IEEE ITW*, Jan. 2010.
- [15] C. Suh and K. Ramchandran, “Exact regeneration codes for distributed storage repair using interference alignment,” in *Proc. 2010 IEEE Int. Symp. on Inform. Theory (ISIT)*, Seoul, Korea, Jun. 2010.
- [16] N. B. Shah, K. V. Rashmi, P. V. Kumar, and K. Ramchandran, “Interference alignment in regenerating codes for distributed storage: necessity and code constructions,” Sep. 2010. Preprint Available online at <http://arxiv.org/abs/1005.1634>.
- [17] Y. Wu, “A construction of systematic MDS codes with minimum repair bandwidth,” Submitted to *IEEE Transactions on Information Theory*, Aug. 2009. Preprint available at <http://arxiv.org/abs/0910.2486>.
- [18] V. Cadambe, S. Jafar, and H. Maleki, “Distributed data storage with minimum storage regenerating codes - exact and functional repair are asymptotically equally efficient,” in *2010 IEEE Intern. Workshop on Wireless Network Coding (WiNC)*, Apr. 2010.
- [19] C. Suh and K. Ramchandran, “On the existence of optimal exact-repair MDS codes for distributed storage,” Apr. 2010. Preprint available at <http://arxiv.org/abs/1004.4663>
- [20] K. Rashmi, N. B. Shah, and P. V. Kumar, “Optimal exact-regenerating codes for distributed storage at the MSR and MBR points via a product-matrix construction,” submitted to *IEEE Transactions on Information Theory*. Preprint available at <http://arxiv.org/pdf/1005.4178>.
- [21] I. Tamo, Z. Wang, and J. Bruck, “MDS Array Codes with Optimal Rebuilding,” to appear in *2011 IEEE Symposium on Information Theory (ISIT)*. Preprint available at <http://arxiv.org/abs/1103.3737>
- [22] V. R. Cadambe, C. Huang, and J. Li, “Permutation codes: optimal exact-repair of a single failed node in MDS code based distributed storage systems,” to appear in *2011 IEEE Symposium on Information Theory (ISIT)*.
- [23] V. R. Cadambe, C. Huang, S. A. Jafar, and J. Li, “Optimal repair of MDS codes in distributed storage via subspace interference alignment,” *arxiv pre-print 2011*. Preprint available at <http://arxiv.org/abs/1106.1250>.

- [24] K. W. Shum and Y. Hu, "Exact minimum-repair-bandwidth cooperative regenerating codes for distributed storage systems," to appear in *2011 IEEE Symposium on Information Theory (ISIT)*. Preprint available at <http://arxiv.org/abs/1102.1609>.
- [25] B. Nazer, S. A. Jafar, M. Gastpar, and S. Vishwanath, "Ergodic interference alignment," in *Proc. 2009 IEEE Symposium on Information Theory (ISIT)*, pp.1769-1773, Jun. 2009
- [26] D. S. Papailiopoulos and A. G. Dimakis, "Distributed storage Codes through Hadamard designs," to appear in *ISIT, 2011*.
- [27] R. Lidl and H. Niederreiter, *Finite Fields (Encyclopedia of Mathematics and its Applications)*, Cambridge Univ. Press, 2008.
- [28] G. Bresler and D. N. C. Tse, "3 User interference channel: Degrees of freedom as a function of channel diversity," *47th Allerton Conf. on Comm. Control and Comp.*, pp.265-271, Sep. 2009
- [29] T. Ho, R. Koetter, M. Mard, M. Effros, J. Shi, and D. Karger, "A random linear network coding approach to multicast," *IEEE Trans. on Inform. Theory*, vol. 52, pp. 4413 – 4430, Oct. 2006.
- [30] R. Motwani and P. Raghavan, *Randomized Algorithms*, Cambridge Univ. Press, 1995.